Estimates for practical quantum cryptography

Norbert Lütkenhaus
Helsinki Institute of Physics, PL 9, FIN-00014 Helsingin yliopisto, Finland
(February 1, 2008)

In this article I present a protocol for quantum cryptography which is secure against attacks on individual signals. It is based on the Bennett-Brassard protocol of 1984 (BB84). The security proof is complete as far as the use of single photons as signal states is concerned. Emphasis is given to the practicability of the resulting protocol. For each run of the quantum key distribution the security statement gives the probability of a successful key generation and the probability for an eavesdropper's knowledge, measured as change in Shannon entropy, to be below a specified maximal value.

03.67.Dd, 03.65.Bz, 42.79.Sz

I. INTRODUCTION

Quantum Cryptography is a technique for generating and distributing cryptographic keys in which the secrecy of the keys is guaranteed by quantum mechanics. The first such scheme was proposed by Bennett and Brassard in 1984 (BB84 protocol) [1]. Sender and receiver (conventionally called Alice and Bob) use a quantum channel, which is governed by the laws of quantum mechanics, and a classical channel which is postulated to have the property that any classical message sent will be faithfully received. The classical channel will also transmit faithfully a copy of the message to any eavesdropper, Eve. Along the quantum channel a sequence of signals is sent chosen at random from two pairs of orthogonal quantum states. Each such pair spans the same Hilbert space. For example, the signals can be realized as polarized photons: one pair uses horizontal and vertical linear polarization (+) while the other uses linear polarization rotated by 45 degrees (×). Bob at random one of two measurements each performing projection measurements on the basis + or ×. The *sifted key* [2] consists of the subset of signals where the bases of signal and measurement coincide leading to deterministic results. This subset can be found by exchange of classical information without revealing the signals themselves. Any attempt of an eavesdropper to obtain information about the signals leads to a non-zero expected error rate in the sifted key and makes it likely that Alice and Bob can detect the presence of the eavesdropper by comparing a subset of the sifted key over the public channel. If Alice and Bob find no errors they conclude (within the statistical bounds of error detection) that no eavesdropper was active. They then translate the sifted key into a sequence of zeros and ones which can be used, for example, as a one-time pad in secure communication.

Several quantum cryptography experiments have been performed. In the experimental set-up noise is always present leading to a bit error rate of, typically, 1 to 5 percent errors in the sifted key [3–6]. Alice and Bob can not even in principle distinguish between a noisy quantum channel and the signature of an eavesdropper activity. The protocol of the key distribution has therefore to be amended by two steps. The first is the *reconciliation* (or error correction) step leading to a key shared by Alice and Bob. The second step deals with the situation that the eavesdropper now has to be assumed to be in the possession of at least some knowledge about the reconciled string. For example, if one collects some parity bits of randomly chosen subsets of the reconciled string as a new key then the Shannon information of an eavesdropper on that new, shorter key can be brought arbitrarily close to zero by control of the number of parity bits contributing towards it. This technique is the generalized privacy amplification procedure by Bennett, Brassard, Crépeau, and Maurer [7].

The final measure of knowledge about the key used in this article is that of change of Shannon entropy. If we assign to each potential key x an a-priori probability $p(x)$ then the Shannon entropy of this distribution is defined as

$$S\left[p(x)\right] = -\sum_x p(x)\log p(x)\ . \tag{1}$$

Note that all logarithms in this article refer to basis 2. The knowledge Eve obtains on the key may be denoted by k and leads to an a-posteriori probability distribution $p(x|k)$. The difference between the Shannon entropy of the a-priori and the a-posteriori probability distribution is a good measure of Eve's knowledge:

$$\Delta_S(k) = S\left[p(x)\right] - S\left[p(x|k)\right]\ . \tag{2}$$

For short, we will call $\Delta_S(k)$ the *entropy change*. We recover the Shannon information as the expected value of that difference as

$$I_S = \langle \Delta_S(k) \rangle = \sum_k p(k) \Delta_S(k) \tag{3}$$

where Eve's knowledge k occurs with probability $p(k)$. If we are able to give a bound on $\Delta_S(k)$ for a specific run of the quantum key distribution experiment then this is a stronger statement than a bound a the Shannon information: we guarantee not only security on average but make a statement on a specific key, as required for secure communication.

The challenge for the theory of quantum cryptography is to provide a statement like the following one: If one finds e errors in a sifted key of length $n_{\rm sif}$ then, after error correction under an exchange of $N_{\rm rec}$ bits of redundant information, a new key of length $n_{\rm fin}$ can be distilled on which, with probability $1-\alpha$, a potential eavesdropper achieves an entropy change of less than $\Delta_{\rm tol}$. Here $\Delta_{\rm tol}$ has to be chosen in view of the application for which the secret key is used for. It is not necessary that each realization of a sifted key leads to a secret key; the realization may be rejected with some probability β. In that case Alice and Bob abort the attempt and start anew.

The final goal is to provide the security statement taking into account the real experimental situation. For example, no real channel exist which fulfill the axiom of faithfulness. There is the danger that an eavesdropper can separate Alice and Bob and replace the public channel by two channels: one from Alice to Eve and another one from Eve to Bob. In this separate world scenario Eve could learn to know the full key without causing errors. She could establish different keys with Alice and Bob and then transfer effectively the messages from Alice to Bob. This problem can be overcome by *authentication* [19]. This technique makes it possible for a receiver of a message to verify that the message was indeed send by the presumed sender. It requires that sender and receiver share some secret knowledge beforehand. It should be noted that it is not necessary to authenticate all individual messages sent along the public channel. It is sufficient to authenticate some essential steps, including the final key, as indicated below. In the presented protocol, successful authentication verifies at the same time that no errors remained after the key reconciliation. The need to share a secret key beforehand to accomplish authentication reduces this scheme from a quantum key distribution system to a quantum key growing system: from a short secret key we grow a longer secret key. On the other hand, since one needs to share a secret key beforehand anyway, one can use part of it to control the flow of side-information to Eve during the stage of key reconciliation in a new way. With side-information we mean any classical information about the reconciled key leaking to the eavesdropper during the reconciliation.

Another problem is that in a real application we can not effectively create single photon states. Recent developments by Law and Kimble [8] promise such sources, but present day experiments use dim coherent states, that is coherent pulses with an expected photon number of typically 1/10 per signal. The component of the signal containing two or more photon states, however, poses problems. It is known that an eavesdropper can, by the use of a quantum non-demolition measurement of the total photon number and splitting of signals, learn with certainty all signals containing more than one photon without causing any errors in the sifted key. If Eve can get hold of an ideal quantum channel this will lead to the existence of a maximum value of loss in the channel which can be tolerated [9,10]. It is not known at present whether this QND attack, possibly combined with attacks on the remaining single photons, is the optimal attack but it is certainly pretty strong.

The eavesdropper is restricted in her power to interfere with the quantum signals only by quantum mechanics. In the most general scenario, she can entangle the signals with a probe of arbitrary dimensions, wait until all classical information is transmitted over the public channel, and then make a measurement on the auxiliary system to extract as much information as possible about the key. Many papers, so far, deal only with single photon signals. At present there exists an important claim of a security proof in this scenario by Mayers [11]. However, the protocol proposed there is, up to now, far less efficient than the here proposed one. Other security proofs extend to a fairly wide class of eavesdropping attacks, the coherent attacks [12].

In this paper I will give a solution to a restricted problem. The restriction consists of four points:

- The eavesdropper attacks each signal individually, no *coherent or collective attacks* take place.
- The signal states consist, indeed, of two pairs of orthogonal single photon states so that two states drawn from different pairs have overlap probability 1/2.
- Bob uses detectors of identical detection efficiencies.
- The initial key shared by Alice and Bob is secret, that is the eavesdropper has negligible information about it. Using the part of the key grown in a previous quantum key growing session is assumed to be safe in this sense.

Within these assumptions I give a procedure that leads with some a-priori probability β to a key shared by Alice and Bob. If successful, the key is secure in the sense that with probability $(1-\alpha)$ any potential eavesdropper achieved an

entropy change less than Δ_{tol}. In contrast to all other work on this subject, this procedure takes into account that the eavesdropper does not necessarily transmit single photons to the receiver; she might use multi-photon signals to manipulate Bob's detectors. The procedure presented here might not be optimal, but it is certifiable safe within the four restrictions mentioned before.

It should be pointed out that coherent eavesdropping attacks are at present beyond our experimental capability. Alice and Bob can increase the difficulty of the task of coherent or collective eavesdropping attacks by using random timing for their signals (although here one has to be weary about the error rate of the key) or by delaying their classical communication thereby forcing Eve to store her auxiliary probe system coherently for longer time. There is an important difference between the threat of growing computer power against classical encryption techniques and the growing power of experimental skills in the attack on quantum key distribution: while it is possible to decode today's message with tomorrow's computer in classical cryptography, you can not use tomorrow's experimental skills in eavesdropping on a photon sent and detected today. It is seems therefore perfectly legal to put some technological restrictions on the eavesdropper. This might be, for example, the restriction to attacks on individual system, or even the restriction to un-delayed measurements. For the use of dim coherent states one might be tempted to disallow Eve to use perfect quantum channels and to give her a minimum amount of damping of her quantum channel. The ultimate goal, however, should be to be *able* to cope without those restrictions.

The structure of the paper is as follows. In section II I present the complete protocol on which the security analysis is based. Then, in section III I discuss in more detail the various elements contributing to the protocol. The heart of the security analysis is presented in section IV before I summarize in section V the efficiency and security of the protocol.

II. HOW TO DO QUANTUM KEY GROWING

The protocol presented here is a suitable combination of the Bennett-Brassard protocol, reconciliation techniques and authentication methods. I make use of the fact that Alice and Bob have to share some secret key beforehand. Instead of seeing that as a draw-back, I make use of it to simplify the control of the side-information flow during the classical data exchange. Side-information might leak to Eve in the form of parity bits, exchanged between Alice and Bob during reconciliation, or in the form of knowledge that a specific bit was received correctly or incorrectly by Bob. The side-information could be taken care of this during the privacy amplification step using the results of [13]. Here I present for clarity a new method to avoid any such side-information which correlates Eve's information about different bits (as parity bits do which are typically used in reconciliation) by using secret bits to encode some of the classical communication.

The notation of the variables is guided by the idea that n_x denotes numbers of bits, especially key length at various stage, N_x denotes numbers of secure bits used in different steps of the protocol, β_i denote probabilities of failing to establish a shared key, α_i denote failure probabilities critical to the safety of an established key, while γ denotes the probability that Alice and Bob, unknown to themselves, do not even share a key. Quantities $\overline{x}$ or $\langle x \rangle$ denote expected values of the quantity x.

The protocol steps and their achievements are:

1. Alice sends a sufficient number of signals to Bob to generate a sifted key of length $n_{\rm sif}$.

2. Bob notifies Alice in which time slot he received a signal.

3. Alice and Bob make a "time stamp" allowing them to make sure that the previous step has been completed before they begin the next step. This can be done, for example, by taking the time of synchronized clocks after step 2 and to include this time into the authentication procedure.

4. Alice sends the bases used for the signals marked in the second step to Bob.

5. Bob compares this information with his measurements and announces to Alice the elements of the generalized sifted key of length $n_{\rm sif}$. The generalized sifted key is formed by two groups of signals. The first is the sifted key of the BB84 protocol formed by all those signals which Bob can unambiguously interpret as a deterministic measurement result of a single photon signal state. The second group consists of those signals which are ambiguous as they can not be thought of as triggered by single photon signals. If two of Bob detectors (for example monitoring orthogonal modes) are triggered, then this is an example of an ambiguous signal. The number of these ambiguous signals is denoted by n_D.

   The announcement of this step has to be included into the authentication.

6. Reconciliation: Alice sends, in total, N_{rec} encoded parity-check bits over the classical channel to Bob as a key reconciliation. Bob uses these bits to correct or to discard the errors. During this step he will learn the actual number of errors n_{err}. The probability that an error remains in the sifted key is given by β_1. Depending on the reconciliation scheme, Eve learns nothing in this step, or knows the position of the errors, or knows that Bob received all the remaining bits correctly.

7. From the observed number of errors n_{err} and of ambiguous non-vacuum results n_D Bob can conclude, using a theorem by Hoeffding, that the expected disturbance measure $\overline{\epsilon} = \left\langle \frac{n_{\mathrm{err}}+w_D n_D}{n_{\mathrm{sif}}} \right\rangle$ is, with probability $1-\alpha_1$, below a suitable chosen upper bound $\overline{\epsilon}_{\max}$. With probability $1-\beta_2$ they find a value for α_1 which allows them to continue this protocol successfully. Here w_D is a weight factor fixed later on.

8. Given the upper bound on the disturbance rate $\overline{\epsilon}_{\max}$, Alice and Bob shorten the key by a fraction τ during privacy amplification such that the Shannon information on that final key is below I. The shortening is accomplished using a hash function [19] chosen at random. To make a statement about the entropy change $\Delta_S(k)$ Eve achieved for this particular transmission they observe that this change is with probability $1-\alpha_2$ less than Δ_{tol}. The probability α_2 can be estimated by $\alpha_2 < \frac{I}{\Delta_{\mathrm{tol}}}$.

9. In the last step Alice chooses at random a suitable hash function which she transmits encrypted to Bob using $N_{\mathrm{aut}}/2$ secret bits. Then she hashes with that function her new key, the time from step 3, and the string of bases from step 5 into a short sequence, called the *authentication tag*, The tag is sent to Bob who compares it with the hashed version of his key. If no error was left after the error correction the tags coincide.This step is repeated with the roles of Alice and Bob interchanged. If Bob detects an error rate too high to allow to proceed with the protocol, he does not forward the correct authentication to Alice. The probability Eve could have guessed the secret bits used by Alice or by Bob to encode their hashed message is given by α_3. The probability that a discrepancy between the two versions of the key remains undetected is denoted by γ.

The *probability of detected failure* is β with $\beta < \beta_1 + \beta_2$ and this failure does not compromise the security. In the case of success Alice and Bob can now say that, at worst, with a *probability of undetected failure* (failure of security) of α (with $\alpha < \alpha_1 + \alpha_2 + \alpha_3$) the eavesdropper can achieve an entropy change for the final key which is bigger than Δ_{tol}. The remaining probability γ describes the probability that Alice and Bob do not detect that they do not even share a key.

Note that the final authentication is made symmetric so that no exchange of information over the success of that step is necessary. Otherwise a party not comparing the authentication tags could regard the key as safe in a separate-world scenario. More explanation about the authentication procedure can be found in section III E. The classical information becoming available to Eve during the creation of the sifted key will be taken care of in the calculations of section IV.

The public channel is now used for the following tasks:

- creation of the sifted key, where Eve learns which signals reached Bob and from which signal set each signal was chosen from,
- transmission of encrypted parity check bits, on which Eve learns nothing,
- for bi-directional reconciliation methods: feedback concerning the success of parity bit comparisons (see following section),
- for reconciliation methods which discard errors: the location of bits discarded from the key,
- announcement of the hash function chosen in this particular realization,
- transmission of the encrypted hash function for authentication and of the unencrypted authentication tags.

The main subject of this paper is to give the fraction τ by which the key has to be shortened to match the security target as a function of the upper bound on the disturbance $\overline{\epsilon}_{\max}$. The estimation has to take care of all information available to Eve by a combination of measurements on the quantum channel and classical information overheard on the public channel. This classical information depends on the reconciliation procedure used. The nature of this information might allow Eve to separate the signals into subsets of signals, for example those being formed by the signals which are correctly (incorrectly) received by Bob, and to treat them differently.

The knowledge of the specific hash function is of no use to Eve in construction of her measurement on the signals. This is a result of the assumption that Eve attacks each signal individually and that the knowledge of the hash functions tells Eve only whether a specific bit will count towards the parity bit of a signal subset or not. She only will

learn how important each individual bit is to her. If the bit is not used then it is too late to change the interaction with that bit to avoid unnecessary errors, since the damage by interaction has been done long before. If it is used, then Eve intends to get the best possible knowledge about it anyway. This situation might be different for scenarios which allow coherent attacks.

III. ELEMENTS OF THE QUANTUM KEY GROWING PROTOCOL

In this section I explain in more detail the steps of the quantum key growing protocol. Special attention is given to the security failure probabilities α_i, limiting the security confidence of an established shared key, and to the failure probabilities β_i, limiting the capability to establish a shared key.

A. Generation of the generalized sifted key

Elements of the generalized sifted key are signals which either can be unambiguously interpreted as being deterministicly detected, given the knowledge of the polarization basis, or which trigger more than one detector. We think of detection set-ups where detectors monitor one relevant mode each. Due to loss it is possible to find no photon in any mode. Since Eve might use multi-photon signals we may find photons in different monitored modes simultaneously, leading to ambiguous signals since more than one detector gives a click. Detection of several photons in *one* mode, however, is deemed to be an unambiguous result. (See further discussion in section IV B.) In practice we will not be able to distinguish between one or several photons triggering the detector. The length of the sifted key accumulated in that way is kept fix to be of length $n_{\rm sif}$.

B. Reconciliation

For the reconciliation we have to distinguish two main classes of procedures: one class corrects the errors using redundant information and the other class discards errors by locating error-free subsections of the sifted key. The class of error-correcting reconciliation can be divided in two further subclasses: one subclass uses only uni-directional information flow from Alice to Bob while the second subclass uses an interactive protocol with bi-directional information flow.

The difference between the three approaches with respect to our protocol shows up in the number of secret bits they need to reconcile the string, the length of the reconciled string, and the probability of success of reconciliation. For experimental realization one should think as well of the practical implementation. For example, interactive protocols are very efficient to implement [14]. To illustrate the difference I give examples for the error correction protocols.

The benchmark for efficiency of error correction is the Shannon limit. It gives the minimum number of bits which have to be revealed about the correct version of a key to reconcile a version which is subjected to an error rate e. This limit is achieved for large keys and the error correction probability approaches then unity. The Shannon limit is given in terms of the amount of Shannon information $I_S(e)$ contained in the version of the key affected by the error rate e. For a binary channel, as relevant in our case, this is given by

$$I_S(e) = 1 + e\log e + (1-e)\log(1-e)\ . \tag{4}$$

The minimum number of bits needed, on average, to correct a key of length n affected by the error rate e is then given by

$$n_{\rm min} = n\ \{1 - I_S(e)\}\ . \tag{5}$$

As mentioned before, perfect error correction is achievable only for $n \to \infty$.

1. Linear Codes for error correction.

Linear codes are a well-established technique which can be viewed in a standard-approach as attaching to each k-bit signal a number of $(n-k)$ bits of linearly independent parity-check bits making it in total a n-bit signal. The receiver gets a noisy version of this n-bit signal and can now in a well-defined procedure find the most-likely k-bit signal. Linear codes which will safely return the correct k-bit signal if up to f of the n bits were flipped by the noisy

channel are denoted by $[n, k, d]$ codes (with $d = 2f + 1$). If the signal is affected by more errors then these will be corrected with less than unit probability.

This technique can be used for error correction. Alice and Bob partition their sifted key into blocks of size k. For each block Alice computes the extra $n - k$ parity bits, encodes them with secret bits and sends them via the classical channel to Bob. Bob then corrects his block according to the standard error correction technique. This procedure could be improved, since the $[n, k, d]$ codes are designed to cope with the situation that even the parity bits might be affected by noise. One can partly take advantage of the situation that these bits are transmitted correctly. However, non-optimal performance is not a security hazard.

The search for an optimal linear code is beyond the scope of this paper. To illustrate the problem I present as specific example the code $[512, 422, 21]$. It uses 90 redundant parity bits to protect a block of 422 bits against 10 errors. So how does this linear code perform if we use it to reconcile a string of $n_{\rm sif} = 10128$ bits which are affected by an error rate of 1%? It can be shown that this string will be reconciled with a probability of $(1 - \beta_1) = 0.908$ at an expense of $N_{\rm rec} = 2160$ secret bits. The practical implementation of a code as long as this one is, however, rather problematic from the point of view of computational resources. In comparison, in the Shannon limit we need to use 819 bits for this task.

2. Interactive error correction

An interactive error correction code was presented by Brassard and Salvail in [14]. This code is reported to correct a key with an error rate of 1% and length $n_{\rm sif} = 10000$ at an average expense of $N_{\rm rec} = 933$ bits. No numbers for β_1 are given, but in several tries no remaining error was found. This protocol operates acceptable close to the Shannon limit which tells us that we need at least 808 bits to correct the key.

3. Situation after reconciliation

After reconciliation Alice and Bob share with probability $(1 - \beta_1)$ the same key. The eavesdropper gathered some information from measurements on the quantum channel. The information she gained from listening to the public channel puts her now into different positions depending on the reconciliation protocol. In case errors are discarded, she knows that all remaining bits in the reconciled string were received correctly by Bob during the quantum transmission. If an uni-directional error correction protocol is used, then listening to the public channel during reconciliation does not give Eve any extra hints. The interactive error correction protocol, however, leaks some information to Eve about the position of bits which were received incorrectly by Bob during the quantum protocol. We will have to take this into account later on. There we take the view that Eve knows the positions of all errors exactly.

A difference between correcting and discarding errors is that, naturally, discarding errors will lead to a shorter reconciled string of length $n_{\rm rec} < n_{\rm sif}$, while the length of the key does not change during error correction so that $n_{\rm rec} = n_{\rm sif}$. Common to all schemes is that Alice and Bob know the precise number of errors which occurred (provided the reconciliation worked). When they discard parts of the sifted key they can open up the discarded bits and learn thereby the actual number of errors (although in this case an additional problem of authentication arises), and when they correct errors Bob knows the number of bit-flips he performed during error correction. This is just the number of errors of the sifted key.

Contrary to common belief it is therefore not necessary to sacrifice elements of the sifted key by public comparison to determine or estimate the number of occurred errors.

C. Privacy amplification and the Shannon information on final key

In previous work it has been shown that for typical error rates in an experimental set-up the eavesdropper could gain, on average, non-negligible amount of Shannon information on the reconciled key [15,16]. This means that we can not use it as a secret key right away. Classical coding theory shows a way to distill a final secret key from the reconciled key by the method of privacy amplification [7]. As a practical implementation of the hashing involved, the secret key is obtained by taking $n_{\rm fin}$ parity bits of randomly chosen subsets of the $n_{\rm rec}$ bits of the reconciled string. The choice of the random subsets is made only at that instance and changes for each repetition of the key growing protocol. This shortening of the key to enhance the security of the final key is common to all other approaches that deal with the security of quantum cryptography, for example by Mayers [11] or Biham et al [12]. However, it differs the way to determine the fraction τ by which the key has to be shortened. In the case of individual eavesdropping

attacks we can go via the collision probability as described below [7]. When we consider joint or collective attacks it is not possible to take this approach due to correlation between the signals which possibly allows Eve to gain an advantage by delaying her measurement until she learns to know the specific parity bits entering the final key.

In the first step we give the main formulas of privacy amplification and introduce the parameter $\tau_1(\overline{\epsilon})$. This parameter indicates the fraction by which the key has to be shortened such that the *expected* eavesdropping information on the final key is less than 1 bit of Shannon information. It is given as a function of Eve's acquired *collision probability*. Any additional bit by which the key is shortened leads to an exponential decrease of that expected Shannon information.

We denote by z the final key of length $n_{\rm fin}$, by x the reconciled key of length $n_{\rm rec}$ and by y the accumulated knowledge of the eavesdropper due to her interaction with the signals and the overheard classical communication via the public channel. We keep separately the *hash function* g which, for example, describes the subsets whose parity bits form the final key. This hash function is part of Eve's knowledge in each realization. Eve's knowledge is expressed in a probability distribution $p(z|g,y)$, that is the probability that z is the key given Eve's measurement results and side-information on the key. In a trivial extension of the starting equation of [7] we find that the Shannon information $\tilde{I}$, averaged over the hash functions, is bounded by

$$I \equiv \langle \tilde{I} \rangle_g \leq n_{\rm fin} + \log \langle p_c^z(g,y) \rangle_{y,g} \tag{6}$$

with the collision probability on the final key defined as $p_c^z(g,y) = \sum_z p^2(z|g,y)$. The collision probability $\langle p_c^z(g,y) \rangle_g$ on the final key, averaged with respect to g, is bounded by the collision probability $p_c^x(y) = \sum_x p^2(x|y)$ on the reconciled key as

$$\langle p_c^z(g,y) \rangle_g < 2^{-n_{\rm fin}} \left(2^{n_{\rm fin}} p_c^x(y) + 1\right) \ . \tag{7}$$

This can be trivially extended to an inequality for $\langle p_c^z(g,y) \rangle_{y,g}$ resulting in

$$\langle p_c(g,y) \rangle_{g,y} < 2^{-n_{\rm fin}} \left(2^{n_{\rm fin}} \langle p_c^x(y) \rangle_y + 1\right) \ . \tag{8}$$

This allows us to give the estimate

$$I \leq \log \left(2^{n_{\rm fin}} \langle p_c^x(y) \rangle_y + 1\right) \tag{9}$$

bounding the eavesdropper's expected Shannon information by her expected collision probability on the sifted key and the length of the final key.

We can reformulate the estimate (9) by introducing the fraction τ_1. If we shorten the reconciled key by this fraction then Eve's expected Shannon information is just one bit on the whole final key. Therefore we find

$$\tau_1 = 1 + \frac{1}{n_{\rm rec}} \log \langle p_c^x(y) \rangle_y \ . \tag{10}$$

We introduce the security parameter n_S as the number of bits by which the final key is shorter than prescribed by the fraction τ_1. This security parameter n_S is implicitly defined by

$$n_{\rm fin} = (1 - \tau_1)\, n_{\rm rec} - n_S \ . \tag{11}$$

With the definitions of τ_1 and n_S we then find [7]

$$I \leq \log(2^{-n_S} + 1) \approx \frac{2^{-n_S}}{\ln 2} \ . \tag{12}$$

From this relation we see that the total amount of Eve's expected Shannon information on the final key decreases exponentially with the security parameter n_S. The main part of this paper will be to estimate $\langle p_c^x(y) \rangle_y$ for various scenarios as a function of the expected disturbance rate $\overline{\epsilon}$ to estimate τ_1 and with that to estimate I as a function $\overline{\epsilon}$.

D. From expected quantities to specific quantities

In the previous section we showed that once we know the expected disturbance rate $\overline{\epsilon}$ and the functional dependence of $\tau_1(\overline{\epsilon})$, we can estimate the eavesdropper's Shannon information I on the final key in dependence of n_S via equation (12). In this section we now show how to link the observed error rate to the expected error rate and how to estimate the entropy change Δ_S in a single run from the expected Shannon information I.

1. From the measured error rate to the expected error rate

Alice and Bob establish a generalized sifted key of length $n_{\rm sif}$. During reconciliation of the sifted key Bob learns the actual number of errors $n_{\rm err}$ of unambiguous signals while he already knows the number n_D of ambiguous signals. Our definition of disturbance is here

$$\epsilon = \frac{n_{\rm err} + w_D n_D}{n_{\rm rec}} \tag{13}$$

with w_D as adjustable weight parameter for ambiguous signals to be chosen in a suitable way. We will present in section IV G a model for which we can choose $w_D = 1/2$. In the case of error correction we have to correct even the ambiguous signals to keep the number $n_{\rm sif}$ fixed and to keep control about the disturbance. The reason is we need to formulate a measure of disturbance per element of the reconciliated key which is bounded. This is possible for correction of errors. In the case of discarding errors the number of errors and ambiguous results per remaining bit is unbounded and we fail to be able to give a bound on $\overline{\epsilon}$ from the measured values.

Therefore we restrict ourselves to the case of corrected errors where we find the length $n_{\rm rec}$ of the reconciled string to be equal to the length $n_{\rm sif}$ of the generalized sifted key. In this situation the measured disturbance is given by $\epsilon_{\rm meas} = \frac{n_{\rm err}+w_D n_D}{n_{\rm sif}}$. Since $n_{\rm sif}$ is kept fixed the expected disturbance is given by $\overline{\epsilon} = \frac{\langle n_{\rm err}+w_D n_D\rangle}{n_{\rm sif}}$. From the measured value $\epsilon_{\rm meas}$ we estimate the average disturbance parameter $\overline{\epsilon}$.

To make the role of $\overline{\epsilon}$ clear it should be pointed out that any given eavesdropping strategy will lead to an expected error probability $\overline{\epsilon}$ while the actually caused and observed error rate can be much lower for an individual run of the protocol. For example, think of an intercept/resend protocol as in [10] where Eve has her lucky day and measures, by chance, all signals in the appropriate bases. This is not very likely, but the treatment presented here takes care of this possibility.

In an application of a theorem by Hoeffding [17], which has been used already in [12], we find an estimate of the number $\langle n_{\rm err} + w_D n_D\rangle$ from the actually measured number $n_{\rm err} + w_D n_D$ for a total number of $n_{\rm sif}$ signals as

$$\langle n_{\rm err} + w_D n_D\rangle < n_{\rm err} + w_D n_D + n_{\rm sif}\delta \tag{14}$$

with probability

$$(1-\alpha_1) > 1 - \exp(-2n_{\rm sif}\delta^2) \tag{15}$$

as long as $w_D \leq 1$. For $w_D \geq 1$ we have to replace equation (15) by $(1-\alpha_1) > 1 - \exp(-\frac{2n_{\rm sif}\delta^2}{w_D^2})$. This means that we can give a bound on the expected disturbance parameter $\overline{\epsilon}$ from the observed quantities n_D and $n_{\rm err}$ within a certain confidence limit. To give a numeric example we choose $w_D = 1/2$ (see section IV G) and refer to the situation reported by Marand and Townsend [3]. There an experiment is presented which can create a sifted key of length $n_{\rm sif} = 1.4\times 10^{-3} n$ from an exchange of n quantum signals at an error rate of 1.2% with a negligible amount of ambiguous signals. Then the choice of $\delta = 0.038$ and a sampling with $n = 10^7$ leads to a reconciled key of length $n_{\rm sif} = 1.4\times 10^4$ with a value of $\alpha_1 \approx 10^{-18}$. This is the probability that the expected disturbance parameter $\overline{\epsilon}$ in a typical realization of the key transfer is less than a maximal value of $\overline{\epsilon}_{\rm max} = 0.05$. The value $\overline{\epsilon}_{\rm max}$ will be used in privacy amplification. An eye has to be kept on the sampling time. With the experiment described in [3] it will take about 10 seconds to establish the sifted key. An example for smaller samples is the choice of $n = 10^5$ and $\delta = 0.4$ which leads for the same system to a reconciled key of length $n_{\rm sif} = 140$ and $\alpha_1 \approx 10^{-19}$, $\overline{\epsilon}_{\rm max} = 0.412$. The probability β_2 to fail to achieve a satisfactory level of confidence at this stage is in most cases negligible in comparison to the failure of reconciliation. It should be noted that these numbers give a rough guidance only, since the experiment does not use single-photon signals.

2. Expected information and information in specific realization

We still need to link the change of Shannon entropy Δ_S on the final key in an *individual* realization of the protocol with a given probability to the Shannon information I, that is over the average over many realizations. The key is thought of as unsafe if the eavesdropper achieves an entropy change bigger than $\Delta_{\rm tol}$ in a specific realization. This happens at most with probability α_2 which is bounded implicitly by $I > \alpha_2\Delta_{\rm tol}$ leading to

$$\alpha_2 < \frac{I}{\Delta_{\rm tol}} = \frac{\log(2^{-n_S}+1)}{\Delta_{\rm tol}} \approx \frac{2^{-n_S}}{\Delta_{\rm tol}\ln 2} \tag{16}$$

So the knowledge of an estimate for I and the prescription of an acceptable value of $\Delta_{\rm tol}$ gives us the probability $1-\alpha_2$ of secrecy of the key.

E. Authentication

The tools of the previous sections allow Alice and Bob to construct a common secret key provided that their classical channel is faithful. Since channels with that property, as such, do not exist, we need to authenticate the procedure to make sure that Alice and Bob actually *share* the new key. Authentication can protect at the same time against errors which survived the reconciliation step and against an eavesdropping attack with a "separate world" approach.

It is essential to make sure that Eve has no influence on the choice of bits entering the generalized sifted key exceeding the power to manipulate the quantum channel. The time-stamp step 3 in the protocol assures us that there is no point in Eve faking the public discussion up to that point since she gained no additional information about the signals so far, especially no information about the polarization basis.

The following sequence of bases for the successful received signals sent from Alice and Bob does not need to be authenticated as well since Eve can not bar corresponding signals from the sifted key without knowing Bob's measurements as well. However, the message describing which bits finally form the generalized sifted key needs to be authenticated since Eve is now in the position to bar signals from the sifted key she shares with Alice by manipulation of the contents of the message [18].

The subsequent reconciliation protocol need not to be authenticated if we authenticate the final key. The reason for that is that the previous steps fixed the reconciled key as the generalized sifted key in Alice's version. If Eve tampers with the reconciliation protocol then Bob will fail correct his key so that it becomes equal to Alice's key. Authentication of the final key will therefore be sufficient to protect against tampering with the public channel in this step. It doubles at the same time to protect against incomplete reconciliation.

To summarize, we need to authenticate the string identifying the elements of the sifted key within the received signals, the time stamp, and the final key. The length of this string is roughly $m \approx 2n_{\rm sif}$. The authentication is done in the following way which is based on the authentication procedure of Wegman and Carter [19]:

Alice chooses a hash-function of approximate length $N_{\rm aut}/2 = 4t \log m$ and sends it encrypted to Bob. Both evaluate the hashed version of the message, the tag, of length t. Alice sends the tag via the public channel to Bob. If the tags coincide then this step is repeated with the role of Alice and Bob interchanged. With this symmetric scheme we make sure that neither Alice nor Bob can be coaxed into a position where they think that authentication succeeded when it in fact failed. The probability that Eve could fake the authentication is given by

$$\alpha_3 = 2^{-t+1} \; . \tag{17}$$

This is at the same time the probability that two distinct final keys lead to the same hashed key. Any remaining error in the final key will therefore lead with probability $1 - \alpha_3$ to a failure of the authentication.

IV. EXPECTED COLLISION PROBABILITY AND EXPECTED ERROR RATE

This section represents the major input of physics to the quantum key growing protocol. The aim is to put an upper bound on the expected average collision probability Eve obtains on the reconciliated key as a function of an average disturbance rate her eavesdropping strategy inflicted on the signals. This is done for two methods of reconciliation, correcting or deleting errors. The result will allow us to give values for the parameter $\tau_1(\overline{\epsilon})$.

A. Collision probability on individual signal

The collision probability on the reconciled key is defined by

$$p_c^x(y) = \sum_x p^2(x|y) \; . \tag{18}$$

We assume that the signal sent by Alice are statistically independent of each other and Eve interacts with and performs measurements on each bit individually. Furthermore, we avoid side-information which correlates signals by the use of secret bits in the reconciliation step. Therefore the conditional probability function $p(x|y)$ for x being the key given Eve's knowledge y factorises into a product of probabilities for each signal. With that the expected collision probability factorises as well into a product of the expected collision probability for each bit. We denote by p_c^x the expected collision probability on one bit so that

$$\langle p_c^x(g,y) \rangle_y = (p_c^x)^{n_{\rm rec}}$$

Furthermore, we denote by the index $\alpha \in \{+, \times\}$ the two conjugate bases (e.g. horizontal or vertical polarization for single photons) used to encode the signals, by $\Psi \in \{0, 1\}$ the logical values, and by k the possible outcomes of Eve's measurement. This leads to an expression of the expected collision probability, at this stage, as

$$p_c^x = \sum_{k,\Psi,\alpha} \frac{p^2(\Psi_\alpha, k_\alpha)}{p(k_\alpha)} \ . \tag{19}$$

We find for the parameter τ_1 describing the shortening of the key during privacy amplification from eqn. (10)

$$\tau_1 = \log(2p_c^x) \ . \tag{20}$$

B. Eve's interaction and detection description

The action of the eavesdropper can be described by a completely positive map [20,21] acting on the signal density matrices ρ as

$$\tilde{\rho} = \sum_k A_k \rho A_k^\dagger \tag{21}$$

where we can associate this interaction with a measurement by Eve of a *Probability Operator Measure* (POM) formed by the operators $F_k = A_k^\dagger A_k$. The operators A_k are arbitrary operators mapping the Hilbert space of the signals to an arbitrary Hilbert space. The only restriction is that $\sum_k A_k^\dagger A_k$ gives the identity operator of the signal Hilbert space. The probability for occurrence of outcome k is then given by $p(k) = \mathrm{Tr}(\rho F_k)$. The action of Bob's detectors can be described by a POM on the resulting Hilbert space after Eve's interaction. Since the detection POM elements and the signal density operators can be represented by real matrices, we can assume the operators A_k to be represented by real matrices as well.

This does not limit the generality of the approach, since the outcome corresponding to an operator $A_k = A_k^{\mathrm{re}} + iA_k^{\mathrm{im}}$, with real operators A_k^{re} and A_k^{im}, is triggered with probability $\mathrm{Tr}(\rho A_k^{\mathrm{re}\dagger} A_k^{\mathrm{re}}) + \mathrm{Tr}(\rho A_k^{\mathrm{im}\dagger} A_k^{\mathrm{im}})$ and the outcome probabilities for Bob's detection, corresponding to POM element F if outcome k of Eve's measurement is being triggered, is given by $\mathrm{Tr}(A_k^{\mathrm{re}} \rho A_k^{\mathrm{re}\dagger} F) + \mathrm{Tr}(A_k^{\mathrm{re}} \rho A_k^{\mathrm{re}\dagger} F)$. Since no cross-terms mixing A_k^{re} and A_k^{im} occur this means that using the two real operators A_k^{re} and A_k^{im}, instead of $A_k = A_k^{\mathrm{re}} + iA_k^{\mathrm{im}}$, will not change the outcome probabilities of Bob's detectors but refines Eve's measurement.

Two typical detection set-ups are shown in figure 1. The active version consists of a polarization analyzer (two detectors monitoring each an output of a polarizing beam-splitter) and a phase shifter which effectively changes the polarization basis of the subsequent measurement. Here one has actively to choose the polarization basis of the measurement. The passive device uses two polarization analyzers, one for each basis, and uses a beam-splitter to split the incoming signal the two polarization analyzers are used with equal probability for detection.

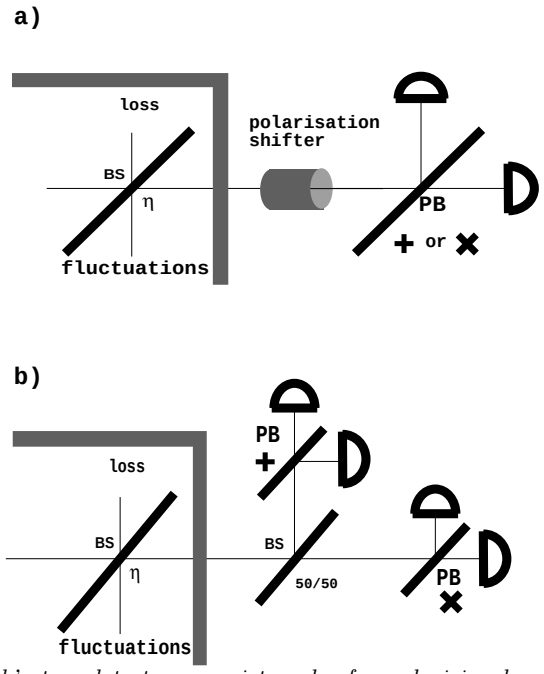

FIG. 1. **(a) Active device:** *Bob's two detectors consist each of a polarizing beam splitter and an ideal detector. The polarizing beam splitter discriminates the two orthogonal linear polarized modes. Using a polarization shifter the polarization basis can be changed as desired. Detector efficiencies are modeled by a beam splitter which represents the loss and which is thought of as being part of the eavesdropper's strategy. This beam splitter can be seen as part of the quantum channel.* **(b) Passive device:** *Here one uses two detection modules as presented in (a), one for each polarization basis. The central beam-splitter takes the task to "switch" between the two polarization analyzers.*

One can represent the detectors by beam-splitters combined with ideal detectors [22]. Then the beam-splitters can be thought to be responsible for the finite efficiency. Since all detectors are assumed to be equal, the losses of all detectors involved can be attributed to a single loss beam-splitter, which is then thought of as being part of the transmission channel rather than being part of the detection unit.

We can use the idea of ideal detectors which measure each a POM with two elements, the projection operator onto the vacuum (no "click") and the projection on the Fock-subspaces with at least one photon ("click"). The POM of the active and the passive set-up then contains the elements $F_{\rm vac}$, F_{0_+}, F_{1_+}, $F_{0_\times}$, $F_{1_\times}$, F_D. These are projections onto the vacuum, $F_{\rm vac}$, onto states with at least one photon in one of the four signal polarizations and none in the others, therefore leading to an unambiguous result, F_{Ψ_α}, and onto the rest of the Hilbert space, that is onto all states containing at least one photon in the signal polarization and at least one in an orthogonal mode F_D. The first POM outcome manifests itself in no detector click at all, the following four give precisely one detector click, and the last one gives rise to at least two detectors being triggered. If we denote by $|n,m\rangle_\alpha$ the state which has n photons in one mode and m photons in the orthogonal polarization mode with respect to the polarization basis α, use the abbreviation $E^{(0)}$ for the projector onto the vacuum and $E^{(n)}_{\Psi_\alpha}$ for the projector onto the state with n photons in the polarization mode corresponding to Ψ_α, then the POM of detection unit (a) is given by

$$\begin{aligned} F_{\rm vac} &= E^{(0)} \\ F_{\Psi_\alpha} &= \frac{1}{2}\sum_{n=1}^{\infty} E^{(n)}_{\Psi_\alpha} \\ F_D &= \frac{1}{2}\sum_{n,m=1}^{\infty} |n,m\rangle_+\langle n,m| + \frac{1}{2}\sum_{n,m=1}^{\infty} |n,m\rangle_\times\langle n,m| \ . \end{aligned} \tag{22}$$

On the other hand, the passive detection scheme (b) is more susceptible to signals containing more than one photon. It is described by the POM

$$\begin{aligned} F_{\rm vac} &= E^{(0)} \\ F_{\Psi_\alpha} &= \sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n E^{(n)}_{\Psi_\alpha} \end{aligned} \tag{23}$$

$$F_D = \sum_{n=1}^{\infty} \left[\left(\frac{1}{2} - \left(\frac{1}{2} \right)^n \right) \sum_{\Psi,\alpha} E^{(n)}_{\Psi,\alpha} \right] + \frac{1}{2} \sum_{n,m=1}^{\infty} |n,m\rangle_+\langle n,m| + \frac{1}{2} \sum_{n,m=1}^{\infty} |n,m\rangle_\times\langle n,m| \; .$$

The next idea concerns all detection set-ups where all elements of the POM commute with the projections E_n onto the subspaces of total photon number n. In that case we find that Bob's measurement on the final signal gives outcome $i \in \{\text{vac}, \Psi_\alpha, D\}$ with probability

$$P_{\text{Bob}}(i) := \text{Tr}(\sum_k A_k \rho A_k^\dagger F_i) = \text{Tr}(\sum_{k,n} E_n A_k \rho A_k^\dagger E_n F_i)$$

We can now replace the set of A_k's by the set $A_{n,k} := E_n A_k$ which still describes Eve measurement but for which each element maps the Hilbert space of the signals to a Hilbert space with a fixed photon number. Eve will now associate a POM element of her measurement with each such $A_{n,k}$ thereby refining her POM and leading to an increase of her knowledge. For short we write again A_k for this set, for which now the property is assumed that the signal arriving at Bob's detection unit is an eigenstate of the total photon number operator. We can divide the index set K of k into subsets $K^{(n)}$ so that for each $k \in K^{(n)}$ the operator A_k maps the one-photon Hilbert space of the signal into the n-photon space. This is useful to distinguish contributions of signals with different photon number.

We still have to discuss how to represent a delayed measurement in this picture. A delayed measurement is performed in the way that Eve brings an auxiliary system into contact with the signal so that they evolve together under a controlled unitary evolution. Then the signal is measured by Bob while Eve delays the measurement of her auxiliary system until she has received all classical information exchanged over the public channel. Having this knowledge, she picks the optimal measurement to be performed on her auxiliary system. Classical information useful to Eve is information that allows her to divide the signals into subsets which should experience different treatment. In our situation this information is represented by the polarization basis of the signal and, for bi-directional error correction, by the knowledge whether the signal was received correctly by Bob. We have therefore to assume, for example, that Eve's delayed measurement is characterized by the set of operators A_k with $k \in K$, giving rise to Eve's POM $F_k = A_k A_k^\dagger$, and which are applied to the signals from the set $\alpha =$ "+" and a second set $B_{k'}$ with $k' \in K'$, resulting in the POM $F'_{k'} = B_{k'} B_{k'}^\dagger$, which are applied to the signals from the set $\alpha =$ "×". Of course, these two sets of operators can not be chosen arbitrarily. The complete positive map has to be identical for all density matrices ρ, that is

$$\tilde{\rho} = \sum_{k \in K} A_k \rho A_k^\dagger = \sum_{k' \in K'} B_{k'} \rho B_{k'}^\dagger \; . \tag{24}$$

Moreover, this equality holds even for non-Hermitian matrices ρ. We can combine this result with the partition into n-photon subspaces. Then we find that even the stronger statement

$$\sum_{k \in K^{(n)}} A_k \rho A_k^\dagger = \sum_{k' \in K'^{(n)}} B_{k'} \rho B_{k'}^\dagger \; . \tag{25}$$

holds. Before we go on to the derivation of the relation between average disturbance and average collision probability I would like to point out that this treatment takes into account the rich structure of modes supported by optical fibers and the fact that detectors monitor a multitude of modes. As long as the detection POM commutes with the projector onto the actually used signal mode, which is usually the case, we can separate the action of the A_k with respect to the photon number in a similar way.

C. Separation into n-photon contributions

In this section we are going to present the disturbance measure ϵ and the collision probability p_c^x as sums over contributions with different definite photon number n arriving at Bob's detector unit. We start from the definition of the disturbance ϵ. To allow some comparison between correcting and discarding errors, we present a unified definition which defines, even for discarded errors, a disturbance measure per bit of the reconciled key. This definition is given by

$$\epsilon = \frac{n_{\rm err} + w_D n_D}{n_{\rm rec}} \ . \tag{26}$$

Here $n_{\rm err}$ is the number of errors in the sifted key, n_D is the number of ambiguous results occurring and $n_{\rm rec}$ is the number of bits in the reconciled string. The weight parameter w_D for ambiguous signals will be fixed later on. If we keep the size of the reconciled key fixed, then the expectation value of ϵ is described by

$$\overline{\epsilon} = \frac{p_{\rm err} + w_D p_D}{p_{\rm rec}} \tag{27}$$

where $p_{\rm err}, p_D, p_{\rm rec}$ are the absolute probabilities that a signal will, respectively, enter the sifted key as error, cause an ambiguous result, or become an element of the reconciled key. As mentioned before, it should be noted, that no estimate $\overline{\epsilon}$ from measured data can be easily presented in the case of discarded errors. We separate the contributions from the different photon number signals as

$$\overline{\epsilon} = \sum_n \frac{p^{(n)}_{\rm rec}}{p_{\rm rec}} \frac{p^{(n)}_{\rm err} + w_D p^{(n)}_D}{p^{(n)}_{\rm rec}} = \sum_n \frac{p^{(n)}_{\rm rec}}{p_{\rm rec}} \overline{\epsilon}^{(n)} \ . \tag{28}$$

where we have implicitly defined

$$\overline{\epsilon}^{(n)} = \frac{p^{(n)}_{\rm err} + w_D p^{(n)}_D}{p^{(n)}_{\rm rec}} \tag{29}$$

as the n-photon contribution towards the disturbance measure. Now $p^{(n)}_X$ are the conditional probabilities that a signal has property X while being transfered as n-photon signal between Eve and Bob. The total disturbance is given as sum over the n-photon contribution weighted by the relative probability that a signal arriving as an n-photon signal at Bob's detector will enter the reconciled key.

If we discard errors, then we find for the relevant probabilities (with $\overline{\Psi}$ as the complement to binary value Ψ)

$$p^{(n)}_{\rm err} = \frac{1}{4} \sum_{\substack{k \in K^{(n)} \\ \Psi,\alpha,}} {\rm Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger F^{(n)}_{\overline{\Psi}_\alpha} \right) \tag{30}$$

$$p^{(n)}_{\rm rec} = \frac{1}{4} \sum_{\substack{k \in K^{(n)} \\ \Psi,\alpha,}} {\rm Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger F^{(n)}_{\Psi_\alpha} \right) \tag{31}$$

$$p^{(n)}_{D} = \frac{1}{4} \sum_{\substack{k \in K^{(n)} \\ \Psi,\alpha,}} {\rm Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger F^{(n)}_{D} \right) \ . \tag{32}$$

If we correct errors, then the probability for a signal to enter the reconciled key differs from equation (31) and is, instead, given by

$$\begin{aligned} p^{(n)}_{\rm rec} &= \frac{1}{4} \sum_{\substack{k \in K^{(n)} \\ \Psi,\alpha,\Psi'}} {\rm Tr}\left(A_k \rho_{\Psi'_\alpha} A_k^\dagger F^{(n)}_{\Psi_\alpha} \right) \\ &= \frac{1}{4} \sum_{\substack{k \in K^{(n)} \\ \Psi,\alpha}} {\rm Tr}\left(A_k A_k^\dagger F^{(n)}_{\Psi_\alpha} \right) \ . \end{aligned} \tag{33}$$

The collision probability is split into contributions related to fixed photon numbers arriving at Bob's detector in the same manner as the disturbance measure to give

$$p^x_c = \sum_{n=1}^{\infty} \frac{p^{(n)}_{\rm rec}}{p_{\rm rec}} p^{(n)}_c \tag{34}$$

with

$$p^{(n)}_c := \sum_{k \in K^{(n)}, \Psi, \alpha} \frac{1}{p^{(n)}_{\rm rec}} \frac{p^2(\Psi_\alpha, k_\alpha)}{p(k_\alpha)} \ .$$

The basic idea is now to estimate the one-photon contributions to these quantities and then to choose w_D in such a way that the optimal eavesdropping strategy will necessarily employ only one-photon signals. To achieve this we will use the fact that multi-photon signals lead unavoidably to ambiguous signals, that is $p_D^{(n)} \neq 0$ for $n > 2$ when using the passive detection option.

D. The one-photon contribution for discarded errors

We use the description of the general eavesdropping strategy to calculate the one-photon contributions. We find with the help of the identity $F_{\Psi_\alpha}^{(1)} = \frac{1}{2}\rho_{\Psi_\alpha}$

$$\begin{aligned} p_c^{(1)} = &\frac{1}{8}\sum_{k\in K^{(1)}} \frac{1}{p_{\rm rec}^{(1)}} \left\{ \frac{{\rm Tr}^2\left(A_k\rho_{0_+}A_k^\dagger\rho_{0_+}\right) + {\rm Tr}^2\left(A_k\rho_{1_+}A_k^\dagger\rho_{1_+}\right)}{{\rm Tr}\left(A_k\rho_{0_+}A_k^\dagger\rho_{0_+}\right) + {\rm Tr}\left(A_k\rho_{1_+}A_k^\dagger\rho_{1_+}\right)} \right\} \\ &+\frac{1}{8}\sum_{k'\in K'^{(1)}} \frac{1}{p_{\rm rec}^{(1)}} \left\{ \frac{{\rm Tr}^2\left(B_{k'}\rho_{0_\times}B_{k'}^\dagger\rho_{0_\times}\right) + {\rm Tr}^2\left(B_{k'}\rho_{1_\times}B_{k'}^\dagger\rho_{1_\times}\right)}{{\rm Tr}\left(B_{k'}\rho_{0_\times}B_{k'}^\dagger\rho_{0_\times}\right) + {\rm Tr}\left(B_{k'}\rho_{1_\times}B_{k'}^\dagger\rho_{1_\times}\right)} \right\} \end{aligned} \tag{35}$$

and with the relation between $p_{\rm rec}^{(1)}$ and $\overline{\epsilon}^{(1)}$ from eqn. (29), and $p_{\rm sif}^{(1)} = p_{\rm err}^{(1)} + p_{\rm rec}^{(1)}$ we find

$$p_{\rm rec}^{(1)} = \frac{p_{\rm sif}^{(1)}}{1+\overline{\epsilon}^{(1)}} \tag{36}$$

together with the quantities

$$p_{\rm rec}^{(1)} = \frac{1}{8}\sum_{\substack{k\in K^{(1)}\\ \Psi,\alpha}} \left\{ {\rm Tr}\left(A_k\rho_{\Psi_\alpha}A_k^\dagger\rho_{\Psi_\alpha}\right)\right\} \tag{37}$$

$$p_{\rm sif}^{(1)} = \frac{1}{4}\sum_{k\in K^{(1)}} {\rm Tr}\left(A_kA_k^\dagger\right)\ . \tag{38}$$

The equations (35–38) form the basis for the following calculations. To start with, we decrease the number of free parameters to a handful of real parameters, so that we can optimize Eve's strategy to give an upper bound on $p_c^{(1)}$ as a function of $\overline{\epsilon}^{(1)}$. To do so, we take a new look at the complete positive mapping (21). We define four vectors $\mathbf{A}_{00}, \mathbf{A}_{10}, \mathbf{A}_{01}, \mathbf{A}_{11}$ with the components $k \in K^{(1)}$ given by

$$A_{\Psi,\Psi'}^k = \langle\Psi_+|A_k|\Psi'_+\rangle\ . \tag{39}$$

These vectors are formed by the transition amplitudes from the signal states to the one-photon detection states for each different measurement outcome. They effectively describe not only the complete channel between Alice and Bob but also the complete eavesdropping strategy. With these vectors we can simplify the notation of the expectation values introducing vector products

$$\sum_{k\in K^{(1)}} {\rm Tr}\left(A_k\rho_{\Psi_+}A_k^\dagger\rho_{\Psi'_+}\right) = \mathbf{A}_{\Psi,\Psi'}\mathbf{A}_{\Psi,\Psi'} = |\mathbf{A}_{\Psi,\Psi'}|^2\ .$$

Similarly we can define vectors $\mathbf{B}_{00}, \mathbf{B}_{10}, \mathbf{B}_{01}, \mathbf{B}_{11}$ and vectors $\tilde{\mathbf{B}}_{00}, \tilde{\mathbf{B}}_{10}, \tilde{\mathbf{B}}_{01}, \tilde{\mathbf{B}}_{11}$ with elements for $k' \in K'^{(1)}$

$$B_{\Psi,\Psi'}^{k'} = \langle\Psi_+|B'_k|\Psi'_+\rangle \tag{40}$$

$$\tilde{B}_{\Psi,\Psi'}^{k'} = \langle\Psi_\times|B'_k|\Psi'_\times\rangle\ . \tag{41}$$

These vectors are not independent. They are related by the identities

$$\tilde{\mathbf{B}}_{00} = \frac{1}{2}\left(\mathbf{B}_{00} - \mathbf{B}_{10} - \mathbf{B}_{01} + \mathbf{B}_{11}\right) \tag{42}$$
$$\tilde{\mathbf{B}}_{01} = \frac{1}{2}\left(\mathbf{B}_{00} - \mathbf{B}_{10} + \mathbf{B}_{01} - \mathbf{B}_{11}\right)$$
$$\tilde{\mathbf{B}}_{10} = \frac{1}{2}\left(\mathbf{B}_{00} + \mathbf{B}_{10} - \mathbf{B}_{01} - \mathbf{B}_{11}\right)$$
$$\tilde{\mathbf{B}}_{11} = \frac{1}{2}\left(\mathbf{B}_{00} + \mathbf{B}_{10} + \mathbf{B}_{01} + \mathbf{B}_{11}\right)$$

The advantage of this description is that the value of any scalar product of the vectors $\mathbf{B}_{\Psi,\Psi'}$ remains unchanged if the $\mathbf{B}_{\Psi,\Psi'}$'s are replaced by $\mathbf{A}_{\Psi,\Psi'}$'s since (25) guarantees that

$$\mathbf{B}_{\Psi,\Psi'}\mathbf{B}_{\phi,\phi'} = \mathbf{A}_{\Psi,\Psi'}\mathbf{A}_{\phi,\phi'} \ . \tag{43}$$

The idea is now to estimate and reformulate the equations (35–38) in such a way that the new set of equations involve only the four vectors $\mathbf{A}_{00}, \mathbf{A}_{10}, \mathbf{A}_{01}, \mathbf{A}_{11}$ and the quantities $\overline{\epsilon}^{(1)}, p_{\rm sif}^{(1)}$ and $p_{\rm rec}^{(1)}$. As a first step we find from eqn. (35)

$$p_c^{(1)} = \frac{1}{8p_{\rm rec}^{(1)}} \sum_{k\in K^{(1)}} \frac{(A_{00}^k)^4 + (A_{11}^k)^4}{(A_{00}^k)^2 + (A_{11}^k)^2} \tag{44}$$
$$+\frac{1}{8p_{\rm rec}^{(1)}} \sum_{k'\in K'^{(1)}} \frac{(\tilde{B}_{00}^{k'})^4 + (\tilde{B}_{11}^{k'})^4}{(\tilde{B}_{00}^{k'})^2 + (\tilde{B}_{11}^{k'})^2} \ ,$$

while equation (36) remains unchanged

$$p_{\rm rec}^{(1)} = \frac{p_{\rm sif}^{(1)}}{1+\overline{\epsilon}^{(1)}} \ . \tag{45}$$

The definitions of $p_{\rm rec}^{(1)}$ and $\overline{\epsilon}^{(1)}$ simplify to

$$p_{\rm rec}^{(1)} = \frac{1}{8}\left(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{11}|^2 + |\tilde{\mathbf{B}}_{00}|^2 + |\tilde{\mathbf{B}}_{11}|^2\right) \tag{46}$$
$$p_{\rm sif}^{(1)} = \frac{1}{4}\left(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{11}|^2 + |\mathbf{A}_{01}|^2 + |\mathbf{A}_{10}|^2\right) \ . \tag{47}$$

Next we use the Cauchy inequality as shown in appendix A to estimate $p_c^{(1)}$ by an expression involving only scalar products of the basic vectors. With use of the definition of $p_{\rm rec}^{(1)}$ this results in the expression

$$p_c^{(1)} \le 1 \tag{48}$$
$$-\frac{1}{4p_{\rm rec}}\frac{(\mathbf{A}_{00}\mathbf{A}_{11})^2}{|\mathbf{A}_{00}|^2 + |\mathbf{A}_{11}|^2} - \frac{1}{4p_{\rm rec}}\frac{\left(\tilde{\mathbf{B}}_{00}\tilde{\mathbf{B}}_{11}\right)^2}{|\tilde{\mathbf{B}}_{00}|^2 + |\tilde{\mathbf{B}}_{11}|^2} \ .$$

We find that there are actually only a few real quantities left. These are $|\mathbf{A}_{00}|, |\mathbf{A}_{11}|$, the angle ϕ_{00}^{11} between $\mathbf{A}_{00}$ and $\mathbf{A}_{11}$, $|\mathbf{A}_{01}|^2 + |\mathbf{A}_{10}|^2$, $|\mathbf{A}_{01} + \mathbf{A}_{10}|^2$, $p_{\rm sif}$ and, finally, $\overline{\epsilon}^{(1)}$. The normalization factor $p_{\rm rec}^{(1)}$ can be immediately eliminated. As shown in appendix B we can optimize $p_c^{(1)}$ and find the result

$$p_c^{(1)} \le \begin{cases} \frac{1}{2}\left(1 + 4\overline{\epsilon}^{(1)} - 4\left(\overline{\epsilon}^{(1)}\right)^2\right) & \text{for } \overline{\epsilon}^{(1)} \le 1/2 \\ 1 & \text{for } \overline{\epsilon}^{(1)} \ge 1/2 \end{cases} \ . \tag{49}$$

To compare this result with other results we introduce the error rate e in the sifted key as $e = \frac{p_{\rm err}^{(1)}}{p_{\rm sif}^{(1)}}$ (so that $\overline{\epsilon}^{(1)} = \frac{e}{1-e}$) and we find

$$p_c^{(1)} \le \frac{1 + 2e - 7e^2}{2\left(1-e\right)^2} \ . \tag{50}$$

This upper bound was given before in [23,24] for the case that Eve performed non-delayed measurements. Recently Slutsky et al. [25,26] have found that this bound holds even for the delayed case. My formulation of that proof shows

that this bound is valid not only for the one-photon contribution but can be extended to include the full Hilbert space of optical fibers and detectors accessible to Eve in real experiments.

From [23,24,26] we know that this bound is sharp since the eavesdropping strategy achieving this bound is given explicitly. It is a translucent attack. An important property of this bound is that for a disturbance rate of $\overline{\epsilon}^{(1)} = \frac{1}{2}$ (or error rate $e = \frac{1}{3}$) the eavesdropping attempt is so successful that each bit of the sifted key originating from this part of the eavesdropping strategy is known with unit probability by Eve.

E. The one-photon contribution for corrected errors

If we correct errors without leaking knowledge about their position to the eavesdropper, then the one photon contribution to the collision probability is given by

$$p_c^{(1)} = \frac{1}{8p_{\rm sif}^{(n)}} \sum_{k\in K^{(1)}} \frac{{\rm Tr}^2(\rho_{0_+} A_k^\dagger A_k) + {\rm Tr}^2(\rho_{1_+} A_k^\dagger A_k)}{{\rm Tr}(A_k^\dagger A_k)} + \frac{1}{8p_{\rm sif}^{(n)}} \sum_{k'\in K'^{(1)}} \frac{{\rm Tr}^2(\rho_{0_\times} B_{k'}^\dagger B_{k'}) + {\rm Tr}^2(\rho_{1_\times} B_{k'}^\dagger B_{k'})}{{\rm Tr}(B_{k'}^\dagger B_{k'})} \ . \tag{51}$$

(Note that $p_{\rm rec}^{(1)} = p_{\rm sif}^{(1)}$.) The disturbance parameter coincides with the error rate $e^{(1)}$ in the sifted key and is given by

$$\overline{\epsilon}^{(1)} = \frac{p_{\rm err}^{(1)}}{p_{\rm sif}^{(1)}} \tag{52}$$

with

$$p_{\rm sif} = \frac{1}{4}\left(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{11}|^2 + |\mathbf{A}_{01}|^2 + |\mathbf{A}_{10}|^2\right) = \frac{1}{4}\left(|\tilde{\mathbf{B}}_{00}|^2 + |\tilde{\mathbf{B}}_{11}|^2 + |\tilde{\mathbf{B}}_{01}|^2 + |\tilde{\mathbf{B}}_{10}|^2\right) \tag{53}$$

$$p_{\rm err} = p_{\rm sif} - \frac{1}{8}\left(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{11}|^2 + |\tilde{\mathbf{B}}_{00}|^2 + |\tilde{\mathbf{B}}_{11}|^2\right) \ . \tag{54}$$

In appendix C I show that the collision probability in this case can be estimated by

$$p_c^{(1)} \leq \begin{cases} \frac{1}{2} + 3\overline{\epsilon}^{(1)} - 5\left(\overline{\epsilon}^{(1)}\right)^2 & \text{for } \overline{\epsilon}^{(1)} \leq 1/4 \\ \frac{3}{4} + \overline{\epsilon}^{(1)} - \left(\overline{\epsilon}^{(1)}\right)^2 & \text{for } 1/4 \leq \overline{\epsilon}^{(1)} \leq 1/2 \\ 1 & \text{for } 1/2 \leq \overline{\epsilon}^{(1)} \end{cases} \ . \tag{55}$$

This estimate is not necessarily sharp, but it is good enough for practical purposes. It shows that $\tau_1 = 1$ for an error rate of $\overline{\epsilon} = 1/2$, which corresponds to a strategy which intercepts and stores all signals while random signals are resent. By delaying the measurement of the signals Eve thus knows all signals while causing a disturbance of 1/2.

F. One-photon contribution for corrected errors with leaked error positions

If Alice and Bob use a bi-directional error correction scheme then Eve will gain some knowledge about the positions of the errors. She can therefore divide the signals into subsets characterized by Eve's measurement outcome k, the polarization basis α of the signal and the correctness of the signal reception of Bob. We therefore need to introduce new operators $C_{\Psi\Psi'}^k$ and $\tilde{D}_{\Psi\Psi'}^k$ to describe the eavesdropping strategy applied to incorrectly received signals. They are formed analogous to $A_{\Psi\Psi'}^k$ and $\tilde{B}_{\Psi\Psi'}^k$ respectively. Then the one-photon contribution towards the collision probability is given by

$$p_c^{(1)} = \frac{1}{8p_{\rm sif}^{(1)}} \sum_{k\in K^{(1)}} \frac{(A_{00}^k)^4 + (A_{11}^k)^4}{(A_{00}^k)^2 + (A_{11}^k)^2} \tag{56}$$

$$+\frac{1}{8p_{\rm sif}^{(1)}} \sum_{k'\in K'^{(1)}} \frac{(\tilde{B}_{00}^{k'})^4 + (\tilde{B}_{11}^{k'})^4}{(\tilde{B}_{00}^{k'})^2 + (\tilde{B}_{11}^{k'})^2} \tag{57}$$

$$+\frac{1}{8p_{\rm sif}^{(1)}} \sum_{k\in K^{(1)}} \frac{(C_{01}^k)^4 + (C_{10}^k)^4}{(C_{01}^k)^2 + (C_{10}^k)^2} \tag{58}$$

$$+\frac{1}{8p_{\rm sif}^{(1)}} \sum_{k'\in K'^{(1)}} \frac{(\tilde{D}_{01}^{k'})^4 + (\tilde{D}_{10}^{k'})^4}{(\tilde{D}_{01}^{k'})^2 + (\tilde{D}_{10}^{k'})^2} \ .$$

The disturbance $\overline{\epsilon}^{(1)}$, $p_{\rm sif}$ and $p_{\rm err}$ are defined as in eqns. (52) to (54) where we note that within scalar products like equation (43) the vectors $\mathbf{C}$ ($\tilde{\mathbf{D}}$) can be replaced by $\mathbf{A}$ ($\tilde{\mathbf{B}}$). In appendix D I show that

$$p_c^{(1)} \leq \begin{cases} \frac{1}{2} + 2\overline{\epsilon}^{(1)} - 2\left(\overline{\epsilon}^{(1)}\right)^2 & \text{for } \overline{\epsilon}^{(1)} \leq 1/2 \\ 1 & \text{for } 1/2 \leq \overline{\epsilon}^{(1)} \end{cases} \ . \tag{59}$$

As it is the case if the error positions are not known to Eve, this estimate is not necessarily sharp. This is due to the use of the Cauchy inequality during the estimation. It shows a behavior analogous to that of equation (55) that for an error rate of $e = 1/2$ (and disturbance rate $\overline{\epsilon} = 1/2$) we find $\tau_1(1/2) = 1$ which means that Eve knows the whole key.

G. Multi-photon signals between Eve and Bob

To deal with multi-photon signals we have to pick a detection model. We will concentrate here on the passive detection scheme to choose w_D such that it is disadvantageous for Eve to use multi-photon signals. In my thesis [23] I have shown that even for active switching between two polarization analyzer with different polarization orientation one can show security against eavesdropping strategies employing multi-photon signals.

The crucial observation for the passive detection unit is that sending multi-photon signals will invariably cause the outcome associated with F_D to appear with a finite probability. This means that we can choose the weight factor w_D such that $\overline{\epsilon}^{(n)} > \overline{\epsilon}^{(1)}$ holds for $n \geq 2$. As a consequence the optimal eavesdropping strategy will employ only single-photon signals. The contribution of ambiguous signals to the disturbance parameter $\overline{\epsilon}^{(n)}$ for discarded errors is bounded by a rough estimate obtained with help of eqn. (23) by omission of suitable positive terms in the expression for F_D

$$\begin{aligned} \frac{p_D^{(n)}}{p_{\rm rec}^{(n)}} &= \frac{\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\alpha}} \mathrm{Tr}(A_k \rho_{\Psi_\alpha} A_k^\dagger F_D)}{\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\alpha}} \mathrm{Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger F_{\Psi_\alpha}^{(n)}\right)} \\ &\geq \frac{\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\alpha}} \left(\frac{1}{2} - 2^{-n}\right) \mathrm{Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger E_{\Psi_\alpha}^{(n)}\right)}{2^{-n}\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\alpha}} \mathrm{Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger E_{\Psi_\alpha}^{(n)}\right)} \\ &= \frac{\left(\frac{1}{2} - 2^{-n}\right)}{2^{-n}} \geq 1 \ . \end{aligned} \tag{60}$$

The contribution of ambiguous signals to the disturbance parameter $\overline{\epsilon}^{(n)}$ for corrected errors is bounded in the same way as

$$\begin{aligned} \frac{p_D^{(n)}}{p_{\rm sif}^{(n)}} &= \frac{\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\alpha}} \mathrm{Tr}(A_k \rho_{\Psi_\alpha} A_k^\dagger F_D)}{\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\Psi',\alpha}} \mathrm{Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger F_{\Psi'_\alpha}^{(n)}\right)} \\ &\geq \frac{\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\Psi',\alpha}} \left(\frac{1}{2} - 2^{-n}\right) \mathrm{Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger E_{\Psi'_\alpha}^{(n)}\right)}{2^{-n}\frac{1}{4}\sum_{\substack{k\in K^{(n)} \\ \Psi,\Psi',\alpha}} \mathrm{Tr}\left(A_k \rho_{\Psi_\alpha} A_k^\dagger E_{\Psi'_\alpha}^{(n)}\right)} \end{aligned} \tag{61}$$

$$= \frac{\frac{1}{4}\left(\frac{1}{2} - 2^{-n}\right)}{2^{-n}\frac{1}{4}} \geq 1 \, .$$

One can find lower values of w_D estimating the expression for $\overline{\epsilon}^{(n)}$ as a whole including the errors in the sifted key. However, the values found here serve our purposes well enough.

For correcting and for discarding errors, we find that a disturbance parameter $\overline{\epsilon} = 1/2$ means that Eve knows the whole key using one-photon signals. Therefore, if we choose $w_D = \frac{1}{2}$ we obtain $\overline{\epsilon}^{(n)} \geq w_D \frac{p_D^{(n)}}{p_{\mathrm{rec}}^{(n)}} \geq \frac{1}{2}$ and $\overline{\epsilon}^{(n)} \geq w_D \frac{p_D^{(n)}}{p_{\mathrm{sif}}^{(n)}} \geq \frac{1}{2}$ respectively and can bound the collision probability, taking into account the possibility of multi-photon signals, for discarded errors by

$$\tau_1(\overline{\epsilon}) \leq \begin{cases} \log\left(1 + 4\overline{\epsilon} - 4\overline{\epsilon}^2\right) & \text{for } \overline{\epsilon} \leq 1/2 \\ 1 & \text{for } 1/2 \leq \overline{\epsilon} \end{cases} \, , \tag{62}$$

for corrected errors without leaked error position by

$$\tau_1(\overline{\epsilon}) \leq \begin{cases} \log\left(1 + 6\overline{\epsilon} - 10\overline{\epsilon}^2\right) & \text{for } \overline{\epsilon} \leq 1/4 \\ \log\left(\frac{3}{2} + 2\overline{\epsilon} - 2\overline{\epsilon}^2\right) & \text{for } 1/4 \leq \overline{\epsilon} \leq 1/2 \\ 1 & \text{for } 1/2 \leq \overline{\epsilon} \end{cases} \, , \tag{63}$$

and for corrected errors with leaked error positions by

$$\tau_1(\overline{\epsilon}) \leq \begin{cases} \log\left(1 + 4\overline{\epsilon} - 4\overline{\epsilon}^2\right) & \text{for } \overline{\epsilon} \leq 1/2 \\ 1 & \text{for } 1/2 \leq \overline{\epsilon} \end{cases} \, . \tag{64}$$

The results for τ_1 are shown in figure 2 and 3 respectively. It should be noted again, that the value of the disturbance parameter changes depending on the intention to correct the errors. For other detector models these results hold as well as long as we can show that for them the condition $\overline{\epsilon}^{(n)} \geq 1/2$ for $n \geq 2$ holds. This condition can be readily satisfied if $p_D^{(n)}/p_{\mathrm{rec}}^{(n)} \geq \mu$ for some $\mu > 0$ and $n \geq 2$ by choosing $w_d = 1/(2\mu)$. For experiments with negligible numbers of ambiguous results we can approximate the disturbance $\overline{\epsilon}$ by a function of $e = \frac{p_{\mathrm{err}}}{p_{\mathrm{sif}}}$ as the traditional error rate in the sifted key. In the case of discarding errors this approximation is $\overline{\epsilon} \approx \frac{e}{1-e}$ while for corrected keys it is $\overline{\epsilon} \approx e$.

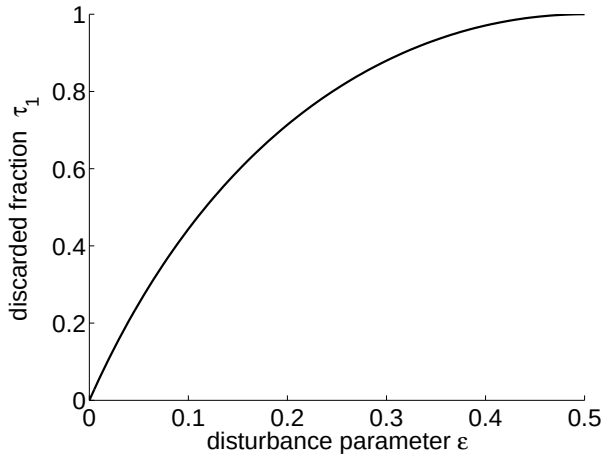

FIG. 2. The fraction τ_1 has to be discarded during privacy amplification as a function of the disturbance per correctly received element of the generalized sifted key if errors are discarded. This result is a sharp estimate in the sense that Eve can reach the level of collision probability on which the estimate is based.

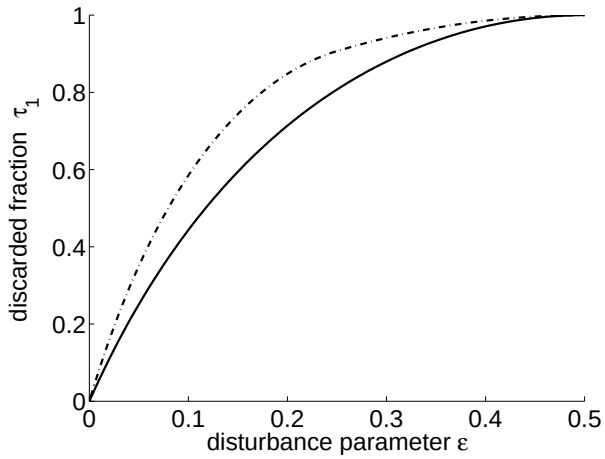

FIG. 3. The fraction τ_1 has to be discarded during privacy amplification as a function of the disturbance per element of the generalized sifted key if one corrects errors. If no information about the position of errors leaked to the eavesdropper, we find for τ_1 the dash-dotted curve, for leaked error positions we find the solid curve.

Since we can not give an estimate for $\overline{\epsilon}$ from measured quantities the case of discarded errors, we concentrate on reconciliation methods which correct errors. From the results of this section we see that this is the better methods anyway, since discarding errors leads to a smaller $n_{\rm rec}$ than correcting errors. This number would have to be reduced further during privacy amplification than in the case of corrected errors, as can be seen by comparison of the estimates for τ_1 as a function of e. Therefore the final key will be shorter and with that the protocol less efficient.

From the estimates we find that the direct estimate for τ_1 gives higher values if the information about error positions has not leaked to the eavesdropper during reconciliation. We can regard the information of error positions as *spoiling information* [7] and thus use the estimate (64) even in the case of uni-lateral error correction. Spoiling information is any information which increases Eve's Shannon information but decreases her expected collision probability on the key leading to a decreased value of τ_1. We conclude that from the point of privacy amplification and reconciliation, the best known way to give a high rate of secure bits would be to use bi-lateral reconciliation methods.

V. ANALYSIS OF THE EFFICIENCY OF KEY GROWING

The process of quantum key growing depends on physical parameters and on the security parameters of the final key. In this section we will bring together the essential formulas about the security statements concerning an accepted key and about the average key growing rate we can expect. This analysis is presented only for error correction reconciliation methods.

A. Security needs

The first thing a potential user has to fix is the tolerated change of Shannon entropy $\Delta_{\rm tol}$ an eavesdropper might obtain on the key without posing a security hazard to the application in mind. Since this limit can not be guaranteed with absolute certainty, the user has to limit the tolerated probability $\alpha_{\rm tol}$ that Eve's knowledge exceeds $\Delta_{\rm tol}$. Authentication may fail to detect errors leaving Alice and Bob with a key neither safe nor shared. The tolerated probability for this has to be specified as $\gamma_{\rm tol}$.

Given $I_{\rm tol}$, $\alpha_{\rm tol}$ and $\gamma_{\rm tol}$ and having in view a particular physical implementation of the quantum channel, Alice and Bob fix a value of the tolerated disturbance $\overline{\epsilon}_{\rm max}$ and of the security bits n_S used in privacy amplification, as well as the length $n_{\rm sif}$ of the sifted key and the number of secure bits $N_{\rm aut}$ used for authentication such that for an accepted key the security target set by $I_{\rm tol}, \alpha_{\rm tol}$ and $\gamma_{\rm tol}$ is met and that the rate of secure bits generated, given below, is optimized.

B. Security statement

The following security statement holds if the key growing is performed by extracting a key of length

$$n_{\rm fin} = n_{\rm sif}\left[1-\tau_1(\overline{\epsilon}_{\rm max})\right] - n_S \tag{65}$$

from the reconciled key during privacy amplification. Here τ_1 is given by by the functional dependence of equations (63) and (64) respectively. From the previous calculations we find that the bits generated in a run of the key growing process are secure in the sense that Eve achieves a change of Shannon entropy on the accepted key of less than $\Delta_{\rm tol}$ with probability α. The contributions to α are the probability of failure of the estimation of the average disturbance given by α_1 in equation (14), the probability to estimate the Shannon information in a specific run from the average information, given by α_2 in equation (16) and the probability of faked authentication, given by α_3 in equation (17). Since all those quantities are expected to be small, the estimate

$$\begin{aligned}\alpha &\leq \alpha_1+\alpha_2+\alpha_3 \\ &= \exp(-2n_{\rm sif}\delta^2) + \frac{\ln(2^{-n_S}+1)}{\Delta_{\rm tol}} + 2^{-N_{\rm aut}+1} \\ &\approx \exp(-2n_{\rm sif}\delta^2) + \frac{2^{-n_S}}{\Delta_{\rm tol}\ln 2} + 2^{-N_{\rm aut}+1}\end{aligned} \tag{66}$$

with $\delta = \overline{\epsilon}_{\rm max} - \epsilon_{\rm meas}$ is sufficient for practical purposes.

The failure to establish a key in a specific run is due to the failure of authentication. Here two contributions can be distinguished. One is the failure of reconciliation, which happens with probability β_1, the other is the failure to reach the target of $\alpha_{\rm tol}$ in that run, which is signaled by making the authentication fail. This happens with a probability β_2. In the design of the set-up and the choice of parameters we would need to estimate β so that at least in the absence of an eavesdropper we will find a net gain of secure bits according to the formula given below. Miscalculation of β does not affect the security of the key, it only affects the efficiency of key generation. We omit therefore detailed examinations of values for β.

The last quantity concerning the security of the key is γ, which is the probability that authentication succeeds although Alice and Bob do not share a key. This probability can be estimated by $\gamma = 2^{-N_{\rm aut}+1}$.

C. Gain

In the previous subsection we described the influence of the chosen basic parameters on the acceptance and security of a run of key growing. Since we need secret bits as an input for the key generation we have to make sure that on average we will gain more secret bits than we put in. The important quantities are here the success probability $p_{\rm succ} = 1-\beta$ that a run of the key expansion leads to accepted new secure bits, the number $N_{\rm out} = n_{\rm rec}\left[1-\tau_1(\overline{\epsilon}_{\rm max})\right] - n_S$ of secret bits gained in that instance and the average number $\overline{N}_{\rm in} = \overline{N}_{\rm rec} + N_{\rm aut}$ of input secret bits. Then the condition for an overall gain on average is to have a positive value of $\overline{N}_{\rm gain} = p_{\rm succ}N_{\rm out} - \overline{N}_{\rm in}$ resulting in

$$\begin{aligned}\overline{N}_{\rm gain} = (1-\beta)\left\{n_{\rm sif}\left[1-\tau_1(\overline{\epsilon}_{\rm max})\right] - n_S\right\} \\ -N_{\rm aut} - N_{\rm rec}\ .\end{aligned} \tag{67}$$

To explore the implications of this condition we go to the limit of large sample sizes. Then we can neglect the number of secret bits used for authentication and and the safety parameter n_S. The remaining contribution of $\overline{N}_{\rm in}$ now comes from the error correction part. For ideal error correction we can set $\beta = 0$ and can use the Shannon limit which gives $\overline{N}_{\rm in} = n_{\rm sif}(1-I_{AB}(\epsilon_{\rm meas}))$ with the Shannon information shared between Alice and Bob given by

$$\begin{aligned}I_{AB}(\epsilon_{\rm meas}) = \\ 1+\epsilon_{\rm meas}\log\epsilon_{\rm meas} + (1-\epsilon_{\rm meas})\log(1-\epsilon_{\rm meas})\ .\end{aligned} \tag{68}$$

With these preparations we find

$$N_{\rm gain} = n_{\rm sif}\left[1-\tau_1(\epsilon_{\rm meas})\right] - n_{\rm sif}(1-I_{AB}(\epsilon_{\rm meas}))\ .$$

In the limit of $n_{\rm sif}\to\infty$ we can assume that $\delta\to 0$ still satisfies any confidence limits put on α. Therefore the condition $\overline{N}_{\rm gain}\geq 0$ is now equivalent to

$$I_{AB}(\epsilon_{\rm meas}) \geq \tau_1(\epsilon_{\rm meas})\ . \tag{69}$$

As we see from figure 4 this means that the protocol in the presented form will be able to grow secret keys only for set-ups operating at an error rate of less than 11.5% for error correction. However, making use of the concept

of spoiling information and of improved estimates of $p_c^{(1)}$ might result in lower estimates for τ_1. A lower bound is, however, the Shannon information I_{AE} shared by Alice and Eve in this scenario. Fuchs et al. give in [15] a sharp bound for I_{AE}, which is shown in figure 4 as dotted line. The difference between τ_1 and I_{AE} represent the average gain G in a run of the key growing protocol in the limit of ideal error correction and infinite sample sizes. The gain

$$G = I_{AB}(\epsilon_{\rm meas}) - \tau_1(\epsilon_{\rm meas}) \tag{70}$$

gives the length of the final key as a fraction of the generalized sifted key.

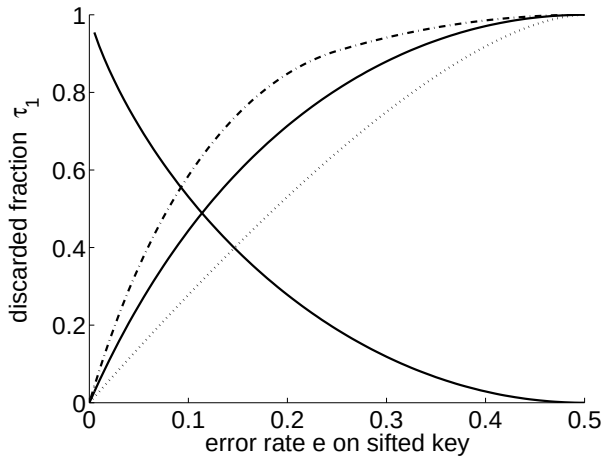

FIG. 4. Shortening during privacy amplification, represented by τ_1 (uni-lateral scenario in dash-dotted curve, bi-lateral scenario as solid curve), in balance with the loss during reconciliation, represented by I_{AB} (falling solid line). The intersections between two lines limits the tolerable error rate in the generalized sifted key in the case of corrected errors. A lower limit of potentially improved bounds for τ_1 is I_{AE} (dotted line).

VI. CONCLUDING REMARKS

In this paper I have given estimates needed in quantum cryptography which are closely oriented towards practical experiments. I do not deal with security against all possible attacks in quantum mechanics, but I deal with all attacks on individual signals. This allows me to include issues related to practical implementation of quantum cryptography which still can not be treated in the general scenario. One of these issues is the question of signals which, for example, triggered simultaneously two detectors monitoring orthogonal polarization modes. (This is the question of multi-photon signals resent by Eve, leading to ambiguous signals.) The other important question is that of an efficient key reconciliation prior to privacy amplification. As seen in this paper it is possible to use the efficient bi-lateral error correction scheme of Brassard and Salvail [14] without compromising security.

In the statistical analysis I showed that it is possible to limit in this scenario the knowledge of the eavesdropper on the final key in a individual realization from *measured quantities* for parameters which seem to be reachable in experiments. As measure of the eavesdropper's knowledge I used the change between a-priori and a-posteriori Shannon entropy associated with the corresponding probability distributions over all possible keys from Eve's point of view. One has to take into account that single photon signals states are not used in today's experiments. However, this theory can be extended to signal states containing multi-photon components. A first approach for that is to estimate $p_c^x = 1$ for each bit of the reconciled key on which Eve could have performed successfully a splitting operation with subsequent delayed measurement. Denote by n_m the total number of these bits, then we need to reduce the key during privacy amplification by

$$\tau_1^{(mult)}(\overline{\epsilon}) = \frac{n_m}{n_{\rm rec}} + \left(1 - \frac{n_m}{n_{\rm rec}}\right) \tau_1 \left(\overline{\epsilon} \frac{n_{\rm rec}}{n_{\rm rec} - n_m}\right) \ . \tag{71}$$

The statistics, however, becomes more complicated this way and it seems to be better to include the dim coherent states directly as signal states and to solve the problem in a clean way. Work in that direction is currently under progress.

The estimates for τ_1 are not necessarily sharp in the case of error correction, and even in the case of discarding errors this limit could be lowered using spoiling information [7]. However, the possible improvement of efficiency of the key growing process is limited and this fine-tuning might be postponed until the experimental relevant situation for dim coherent signal states is solved.

ACKNOWLEDGMENTS

I would like to thank Miloslav Dušek, Richard Hughes, Paul Townsend and the participants of the 1997 workshop on quantum information at the Institute for Scientific Interchange (Italy) for discussions and Steven van Enk for helpful critical comments on the manuscript. For fincancial support I would like to thank Elsag–Bailey and the Academy of Finland. The foundations to this article were laid while I did research for my PhD thesis under supervision and support of Steve Barnett.

APPENDIX A: CAUCHY INEQUALITY

In this appendix we prove the inequality (48) starting from the expression

$$p_c^{(1)} = \frac{1}{8p_{\rm rec}^{(1)}} \sum_{k\in K^{(1)}} \frac{(A_{00}^k)^4 + (A_{11}^k)^4}{(A_{00}^k)^2 + (A_{11}^k)^2} + \frac{1}{8p_{\rm rec}^{(1)}} \sum_{k'\in K'^{(1)}} \frac{(\tilde{B}_{00}^{k'})^4 + (\tilde{B}_{11}^{k'})^4}{(\tilde{B}_{00}^{k'})^2 + (\tilde{B}_{11}^{k'})^2} \,. \tag{A1}$$

We rewrite the first sum as

$$\sum_k \left((A_{00}^k)^2 + (A_{11}^k)^2 - 2\frac{\left(A_{00}^k A_{11}^k\right)^2}{(A_{00}^k)^2 + (A_{11}^k)^2} \right) \tag{A2}$$

and use the Cauchy inequality, given as

$$\left(\sum_k x_k y_k\right)^2 \le \left(\sum_k x_k^2\right)\left(\sum_k y_k^2\right) \tag{A3}$$

or

$$\sum_k x_k^2 \ge \frac{\left(\sum_k x_k y_k\right)^2}{\sum_k y_k^2 \,.} \tag{A4}$$

We set $x_k = \frac{\left(A_{00}^k A_{11}^k\right)}{\sqrt{(A_{00}^k)^2+(A_{11}^k)^2}}$ and $y_k = \sqrt{(A_{00}^k)^2 + (A_{11}^k)^2}$ to obtain the inequality

$$\sum_k \frac{(A_{00}^k)^4 + (A_{11}^k)^4}{(A_{00}^k)^2 + (A_{11}^k)^2} \le \sum_k \left((A_{00}^k)^2 + (A_{11}^k)^2\right) - 2\frac{\left(\sum_k A_{00}^k A_{11}^k\right)^2}{\sum_k (A_{00}^k)^2 + (A_{11}^k)^2} \,. \tag{A5}$$

This can be used to estimate the first part in (A1) while the second part can be estimated similarly so that, with the help of eqn. (46), we find the result

$$p_c^{(1)} \le 1 - \frac{1}{4p_{\rm rec}} \frac{\left(\mathbf{A}_{00}\mathbf{A}_{11}\right)^2}{|\mathbf{A}_{00}|^2 + |\mathbf{A}_{11}|^2} - \frac{1}{4p_{\rm rec}} \frac{\left(\tilde{\mathbf{B}}_{00}\tilde{\mathbf{B}}_{11}\right)^2}{|\tilde{\mathbf{B}}_{00}|^2 + |\tilde{\mathbf{B}}_{11}|^2} \,. \tag{A6}$$

APPENDIX B: MAXIMIZING $P_C^{(1)}$ FOR DISCARDED ERRORS

To optimize the expression (48) we first note that we can assume that $|\mathbf{A}_{00}| = |\mathbf{A}_{11}|$. If Eve starts with a strategy defined by operators A_k not satisfying this condition, then she could use the A-operators $\overline{A}_k = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A_k \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ without a change in the obtained collision probability or disturbance. When we combine the two strategies we find that the resulting vectors satisfy $|\mathbf{A}_{00}| = |\mathbf{A}_{11}|$ and $|\mathbf{A}_{01}| = |\mathbf{A}_{10}|$. This then gives the estimate $|\mathbf{A}_{01} + \mathbf{A}_{10}|^2 \leq 4|\mathbf{A}_{01}|^2$. Another observation is that we can always choose $|\mathbf{A}_{00}| + |\mathbf{A}_{11}| \geq |\tilde{\mathbf{B}}_{00}| + |\tilde{\mathbf{B}}_{11}|$ which means that there are less or equal errors in the sifted key coming from the use of the polarization basis '+' than from the basis '×'. This can be always satisfied, since both polarization basis could be interchanged. Using $|\mathbf{A}_{00}| = |\mathbf{A}_{11}|$ and the definition of $|\tilde{\mathbf{B}}_{00}|$ and $|\tilde{\mathbf{B}}_{11}|$ this results in $2|\mathbf{A}_{00}|^2(1 - \cos\phi_{00}^{11}) \geq |\mathbf{A}_{01} + \mathbf{A}_{10}|^2$ with the angle ϕ_{00}^{11} between $\mathbf{A}_{00}$ and $\mathbf{A}_{11}$.

The three relevant relations now become after elimination of $p_{\text{rec}}^{(1)}$ according to (36) and the use of the relations (42)

$$p_c^{(1)} \leq 1 - \frac{(1+\overline{\epsilon}^{(1)})|\mathbf{A}_{00}|^2(\cos\phi_{00}^{11})^2}{8p_{\text{sif}}} - \frac{(1+\overline{\epsilon}^{(1)})\left(2|\mathbf{A}_{00}|^2(1+\cos\phi_{00}^{11}) - |\mathbf{A}_{01}+\mathbf{A}_{10}|^2\right)^2}{32p_{\text{sif}}\left(2|\mathbf{A}_{00}|^2(1+\cos\phi_{00}^{11}) + |\mathbf{A}_{01}+\mathbf{A}_{10}|^2\right)} \tag{B1}$$

$$\frac{p_{\text{sif}}}{(1+\overline{\epsilon}^{(1)})} = \frac{1}{8}\left(|\mathbf{A}_{00}|^2(3+\cos\phi_{00}^{11}) + \frac{1}{2}|\mathbf{A}_{01}+\mathbf{A}_{10}|^2\right) \tag{B2}$$

$$p_{\text{sif}} = \frac{1}{2}\left(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{01}|^2\right) \tag{B3}$$

Our next step is to show that we can estimate the optimal value of $p_c^{(1)}$ by replacing $|\mathbf{A}_{01} + \mathbf{A}_{10}|^2$ by $4|\mathbf{A}_{01}|^2$. To see that we observe that this would allow to decrease $(1 + \overline{\epsilon}^{(1)})$ by eqn (B2), meaning a lower error rate. At the same time $p_c^{(1)}$ grows indirectly from the falling value of $(1 + \overline{\epsilon}^{(1)})$ and directly, since $\frac{d}{dD}p_c^{(1)} \geq 0$ with $D := |\mathbf{A}_{01} + \mathbf{A}_{10}|^2$. To prove the last point we calculate

$$\frac{d}{dD}p_c^{(1)} = \frac{(1+\overline{\epsilon}^{(1)})\mathcal{A}}{32p_{\text{sif}}\left(2|\mathbf{A}_{00}|^2 + D + 2|\mathbf{A}_{00}|^2\cos\phi_{00}^{11}\right)^2} \tag{B4}$$

$$\mathcal{A} = 12|\mathbf{A}_{00}|^4 - 4|\mathbf{A}_{00}|^2 D - D^2 + 24|\mathbf{A}_{00}|^4\cos\phi_{00}^{11} - 4|\mathbf{A}_{00}|^2 D\cos\phi_{00}^{11} + 12|\mathbf{A}_{00}|^4(\cos\phi_{00}^{11})^2\ . \tag{B5}$$

This is positive, if $\mathcal{A}$ is positive. This is, indeed, the case since

$$\frac{d}{dD}\mathcal{A} = -4|\mathbf{A}_{00}|^2 - 2D - 4|\mathbf{A}_{00}|^2\cos\phi_{00}^{11} \leq 0 \tag{B6}$$

allows us to evaluate $\mathcal{A}$ at the maximal value of $D_{\max} = 2|\mathbf{A}_{00}|^2(1 - \cos\phi_{00}^{11})$ where it gives zero. This proves that $\mathcal{A} \geq 0$ and with that $\frac{d}{dD}p_c^{(1)} \geq 0$. Therefore, three relevant equations become

$$p_c^{(1)} \leq 1 - \frac{(1+\overline{\epsilon}^{(1)})|\mathbf{A}_{00}|^2(\cos\phi_{00}^{11})^2}{8p_{\text{sif}}} - \frac{(1+\overline{\epsilon}^{(1)})\left(|\mathbf{A}_{00}|^2(1+\cos\phi_{00}^{11}) - 2|\mathbf{A}_{01}|^2\right)^2}{16p_{\text{sif}}\left(|\mathbf{A}_{00}|^2(1+\cos\phi_{00}^{11}) + 2|\mathbf{A}_{01}|^2\right)} \tag{B7}$$

$$\frac{p_{\text{sif}}}{(1+\overline{\epsilon}^{(1)})} = \frac{1}{8}\left(|\mathbf{A}_{00}|^2(3+\cos\phi_{00}^{11}) + 2|\mathbf{A}_{01}|^2\right) \tag{B8}$$

$$p_{\text{sif}} = \frac{1}{2}\left(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{01}|^2\right) \tag{B9}$$

We solve (B8) and (B9) for $|\mathbf{A}_{01}|$ and $\cos\phi_{00}^{11}$ and insert these into (B7). The maximum over $|\mathbf{A}_{00}|$ is then taken and we find

$$p_c^{(1)} \leq \frac{1}{2}\left(1 + 4\overline{\epsilon}^{(1)} - 4\left(\overline{\epsilon}^{(1)}\right)^2\right)\ . \tag{B10}$$

The strategy resulting in this collision probability is described by

$$|\mathbf{A}_{00}|^2 = |\mathbf{A}_{11}|^2 = \frac{2p_{\text{sif}}}{1+\overline{\epsilon}^{(1)}} \tag{B11}$$

$$|\mathbf{A}_{01}|^2 = |\mathbf{A}_{10}|^2 = \frac{2p_{\text{sif}}\overline{\epsilon}^{(1)}}{1+\overline{\epsilon}^{(1)}} \tag{B12}$$

$$\cos\phi_{00}^{11} = 1 - 2\overline{\epsilon}^{(1)} \tag{B13}$$

$$\cos\phi_{01}^{10} = 1\ . \tag{B14}$$

In the derivation we have chosen $2|\mathbf{A}_{00}|^2(1-\cos\phi_{00}^{11}) \geq |\mathbf{A}_{01}+\mathbf{A}_{10}|^2$ and find the optimal solution respects this choice for $\overline{\epsilon}^{(1)} \leq \frac{1}{2}$. For $\overline{\epsilon}^{(1)} = \frac{1}{2}$ we find $p_c^{(1)} = 1$ so that we conclude that

$$p_c^{(1)} \leq \begin{cases} \frac{1}{2}\left(1+4\overline{\epsilon}^{(1)}-4\left(\overline{\epsilon}^{(1)}\right)^2\right) & \text{for } \overline{\epsilon}^{(1)} \leq 1/2 \\ 1 & \text{for } \overline{\epsilon}^{(1)} \geq 1/2 \end{cases} . \tag{B15}$$

APPENDIX C: MAXIMIZING $P_C^{(1)}$ FOR CORRECTED ERRORS

We start from equation (51) and use the Cauchy inequality in a similar way as in appendix B. We obtain the bound

$$\begin{aligned} p_c^{(1)} \leq 1 &- \frac{(\mathbf{A}_{00}\mathbf{A}_{10})^2+(\mathbf{A}_{00}\mathbf{A}_{11})^2+(\mathbf{A}_{01}\mathbf{A}_{10})^2+(\mathbf{A}_{01}\mathbf{A}_{11})^2}{\left(|\mathbf{A}_{00}|^2+|\mathbf{A}_{01}|^2+|\mathbf{A}_{10}|^2+|\mathbf{A}_{11}|^2\right)^2} \\ &- \frac{\left(\tilde{\mathbf{B}}_{00}\tilde{\mathbf{B}}_{10}\right)^2+\left(\tilde{\mathbf{B}}_{00}\tilde{\mathbf{B}}_{11}\right)^2+\left(\tilde{\mathbf{B}}_{01}\tilde{\mathbf{B}}_{10}\right)^2+\left(\tilde{\mathbf{B}}_{01}\tilde{\mathbf{B}}_{11}\right)^2}{\left(\left|\tilde{\mathbf{B}}_{00}\right|^2+\left|\tilde{\mathbf{B}}_{01}\right|^2+\left|\tilde{\mathbf{B}}_{10}\right|^2+\left|\tilde{\mathbf{B}}_{11}\right|^2\right)^2} . \end{aligned} \tag{C1}$$

Next we introduce the angles $\varphi_{00}^{11}, \varphi_{00}^{10}, \varphi_{01}^{10}$ between the corresponding vectors $\mathbf{A}_{00}, \mathbf{A}_{10}, \mathbf{A}_{01}, \mathbf{A}_{11}$, make use of the relations (42) and (43), use the symmetry argument as in appendix B and find after some transformation the set of equations

$$\begin{aligned} p_c^{(1)} &\leq \frac{3}{4} \\ &+\frac{|\mathbf{A}_{00}|^4(1-3\cos^2\varphi_{00}^{11})+|\mathbf{A}_{01}|^4(1-3\cos^2\varphi_{01}^{10})}{8(|\mathbf{A}_{00}|^2+|\mathbf{A}_{01}|^2)^2} \\ &+|\mathbf{A}_{00}|^2|\mathbf{A}_{01}|^2\,\frac{3+\cos\varphi_{00}^{11}\cos\varphi_{01}^{10}-2\cos^2\varphi_{00}^{10}}{4(|\mathbf{A}_{00}|^2+|\mathbf{A}_{01}|^2)^2} \end{aligned} \tag{C2}$$

$$\overline{\epsilon}^{(1)} = \frac{|\mathbf{A}_{00}|^2(1-\cos\varphi_{00}^{11})+|\mathbf{A}_{01}|^2(3-\cos\varphi_{01}^{10})}{4(|\mathbf{A}_{00}|^2+|\mathbf{A}_{01}|^2)} \tag{C3}$$

The first observation is that it is optimal to choose $\cos\varphi_{00}^{10} = 0$ since this choice optimizes $p_c^{(1)}$ while it leaves $\overline{\epsilon}^{(1)}$ unchanged. The second observation is that the choice of

$$|\mathbf{A}_{00}|^2\cos\varphi_{00}^{11} = |\mathbf{A}_{01}|^2\cos\varphi_{01}^{10} \tag{C4}$$

within the subspace defined by

$$|\mathbf{A}_{00}|^2\cos\varphi_{00}^{11}+|\mathbf{A}_{01}|^2\cos\varphi_{01}^{10} = const$$

and fixed values of $|\mathbf{A}_{00}|$ and $|\mathbf{A}_{01}|$ is optimal if this choice is possible. In this case we are left with the equations

$$\begin{aligned} p_c^{(1)} &\leq \frac{3}{4} \\ &+\frac{|\mathbf{A}_{00}|^4(1-4\cos^2\varphi_{00}^{11})+|\mathbf{A}_{01}|^4+6|\mathbf{A}_{00}|^2|\mathbf{A}_{01}|^2}{8(|\mathbf{A}_{00}|^2+|\mathbf{A}_{01}|^2)^2} \end{aligned} \tag{C5}$$

$$\overline{\epsilon}^{(1)} = \frac{|\mathbf{A}_{00}|^2(1-2\cos\varphi_{00}^{11})+3|\mathbf{A}_{01}|^2}{4(|\mathbf{A}_{00}|^2+|\mathbf{A}_{01}|^2)} . \tag{C6}$$

At the end of a short maximization calculation we find a solution consistent with symmetry condition (C4) for $\frac{1}{4} \leq \overline{\epsilon}^{(1)} \leq \frac{1}{2}$. It is given by

$$p_c^{(1)} \leq \frac{3}{4}+\overline{\epsilon}^{(1)}-\left(\overline{\epsilon}^{(1)}\right)^2 . \tag{C7}$$

This maximum is obtained by choosing the values $\cos\varphi_{00}^{11} = \frac{1-2\overline{\epsilon}^{(1)}}{2(1-\overline{\epsilon}^{(1)})}$ and $|\mathbf{A}_{01}| = |\mathbf{A}_{00}|\sqrt{\frac{\overline{\epsilon}^{(1)}}{1-\overline{\epsilon}^{(1)}}}$. The symmetry condition (C4) then gives $\cos\varphi_{01}^{10} = \frac{1-2\overline{\epsilon}^{(1)}}{2\overline{\epsilon}^{(1)}}$ which limits the range of validity to $\frac{1}{4} \leq \overline{\epsilon}^{(1)}$. For $\frac{1}{4} \geq \overline{\epsilon}^{(1)}$ we find the optimal solution by selecting $\cos\varphi_{01}^{10} = 1$. A short maximization calculation then gives the bound

$$p_c^{(1)} \leq \frac{1}{2} + 3\overline{\epsilon}^{(1)} - 5\left(\overline{\epsilon}^{(1)}\right)^2 \tag{C8}$$

for the choice of parameters $\cos\varphi_{00}^{11} = \frac{1-3\overline{\epsilon}^{(1)}}{1-\overline{\epsilon}^{(1)}}$ and $|\mathbf{A}_{01}| = |\mathbf{A}_{00}|\sqrt{\frac{\overline{\epsilon}^{(1)}}{1-\overline{\epsilon}^{(1)}}}$.

APPENDIX D: MAXIMIZING $P_C^{(1)}$ FOR CORRECTED ERRORS WITH LEAKED ERROR POSITIONS

We apply Cauchy inequalities to equation (56) and use the vector notations $\mathbf{A}$, $\tilde{\mathbf{B}}$, $\mathbf{C}$, and $\tilde{\mathbf{D}}$ to find

$$\begin{aligned} p_c^{(1)} &\leq 1 \\ &- \frac{1}{4p_{\text{sif}}} \frac{|\mathbf{A}_{00}\mathbf{A}_{11}|^2}{|\mathbf{A}_{00}|^2 + |\mathbf{A}_{11}|^2} - \frac{1}{4p_{\text{sif}}} \frac{|\mathbf{C}_{01}\mathbf{C}_{10}|^2}{|\mathbf{C}_{01}|^2 + |\mathbf{C}_{10}|^2} \\ &- \frac{1}{4p_{\text{sif}}} \frac{\left|\tilde{\mathbf{B}}_{00}\tilde{\mathbf{B}}_{11}\right|^2}{|\tilde{\mathbf{B}}_{00}|^2 + |\tilde{\mathbf{B}}_{11}|^2} - \frac{1}{4p_{\text{sif}}} \frac{\left|\tilde{\mathbf{D}}_{01}\tilde{\mathbf{D}}_{10}\right|^2}{|\tilde{\mathbf{D}}_{01}|^2 + |\tilde{\mathbf{D}}_{10}|^2} . \end{aligned} \tag{D1}$$

It becomes clear immediately that we can replace $\mathbf{C}$ by $\mathbf{A}$ and $\tilde{\mathbf{D}}$ by $\tilde{\mathbf{B}}$ because of relations similar to (43). Similar to the calculations in appendices B and C we introduce the angles $\varphi_{00}^{11}, \varphi_{00}^{10}, \varphi_{01}^{10}$ and use the relations (42) and (43) and the symmetry argument introduced in appendix B to find the new form of (D1) as

$$\begin{aligned} p_c^{(1)} \leq \frac{3}{4} &- \frac{|\mathbf{A}_{00}|^2\cos^2\varphi_{00}^{11} + |\mathbf{A}_{01}|^2\cos^2\varphi_{01}^{10}}{4(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{01}|^2)} \\ &+ \frac{|\mathbf{A}_{00}|^2|\mathbf{A}_{01}|^2}{2(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{01}|^2)} \left[\frac{(1+\cos\varphi_{00}^{11})(1+\cos\varphi_{01}^{10})}{|\mathbf{A}_{00}|^2(1+\cos\varphi_{00}^{11}) + |\mathbf{A}_{01}|^2(1+\cos\varphi_{01}^{10})} + \right. \\ &\left. \frac{(1-\cos\varphi_{00}^{11})(1-\cos\varphi_{01}^{10})}{|\mathbf{A}_{00}|^2(1-\cos\varphi_{00}^{11}) + |\mathbf{A}_{01}|^2(1-\cos\varphi_{01}^{10})}\right] \end{aligned} \tag{D2}$$

while we take from appendix C the expression for $\overline{\epsilon}^{(1)}$ as

$$\overline{\epsilon}^{(1)} = \frac{|\mathbf{A}_{00}|^2(1-\cos\varphi_{00}^{11}) + |\mathbf{A}_{01}|^2(3-\cos\varphi_{01}^{10})}{4(|\mathbf{A}_{00}|^2 + |\mathbf{A}_{01}|^2)} . \tag{D3}$$

We next perform a variation along the path defined by $|\mathbf{A}_{00}|^2\cos\varphi_{00}^{11} + |\mathbf{A}_{01}|^2\cos\varphi_{01}^{10} = const$ and find that $p_c^{(1)}$ is optimized for the choice $\cos\varphi_{00}^{11} = \cos\varphi_{01}^{10}$. An optimization calculation for the remaining parameters leads to the estimate

$$p_c^{(1)} \leq \frac{1}{2} + 2\overline{\epsilon}^{(1)} - 2\left(\overline{\epsilon}^{(1)}\right)^2 \tag{D4}$$

for a disturbance $\overline{\epsilon}^{(1)} \leq 1/2$. This optimum is obtained by choosing $\cos\varphi_{00}^{11} = 1 - 2\overline{\epsilon}^{(1)}$ and $|\mathbf{A}_{00}| = |\mathbf{A}_{01}|\sqrt{\frac{1-\overline{\epsilon}^{(1)}}{\overline{\epsilon}^{(1)}}}$.

[1] C. H. Bennett and G. Brassard, In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, (IEEE, New York, 1984) pp. 175–179.

[2] B. Huttner and A. K. Ekert, J. Mod. Opt. **41,** 2455–2466 (1994).

[3] C. Marand and P. T. Townsend, Opt. Lett. **20,** 1695–1697 (1995).

[4] H. Zbinden, N. Gisin, B. Huttner, A. Muller, J. Cryptol. **11,** 1–14 (1998).
[5] J. D. Franson and H. Ilves, J. Mod. Opt. **41,** 2391–2396 (1994).
[6] W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. A **57,** 2379–2382 (1998).
[7] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theo. **41,** 1915 (1995).
[8] C. K. Law and H. J. Kimble, J. Mod. Opt. **44,** 2067–2074 (1997).
[9] H. P. Yuen, Quantum. Semicl. Opt. **8,** 939–949 (1996).
[10] B. Huttner and N. Imoto and N. Gisin and T. Mor, Phys. Rev. A **51,** 1863–1869 (1995).
[11] D. Mayers, Report quant-ph/9802025, (1998).
[12] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Report quant-ph/9801022, (1998).
[13] C. Cachin and U. M. Maurer, J. Crypt. **10,** 97–110 (1997).
[14] G. Brassard and L. Salvail, In *Proceedings of Eurocrypt '93, held in Lofthus, Norway, 1993*,
[15] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56,** 1163–1176 (1997).
[16] N. Lütkenhaus, Phys. Rev. A **54,** 97 (1996).
[17] W. Hoeffding, J. Amer. Stat. Ass **58,** 13–30 (1963).
[18] In an earlier version of this paper I omitted the authentication of this step. I am grateful to Miloslav Dušek for pointed out to me the danger arising from that.
[19] M. N. Wegman and J. L. Carter, J. Comp. Syst. Sci. **22,** 265–279 (1981).
[20] E. B. Davies, *Quantum Theory of Open Systems* (Academic Press, London, New York, San Francisco, 1976).
[21] K. Kraus, in *States, Effects, and Operations*, No. 190 in *Lecture Notes in Physics*, A. Böhm, J. D. Dollard, and W. Wooters, eds., (Springer, Berlin, 1983).
[22] B. Yurke, Phys. Rev. A **32,** 311–323 (1985).
[23] N. Lütkenhaus, Ph.D. thesis, University of Strathclyde, Glasgow, Scotland, 1996.
[24] N. Lütkenhaus and S. M. Barnett, In *Proceedings of an International Workshop on Quantum Communication, Computing, and Measurement, held September 25-30 in Shizuoka, Japan*, O. Hirota, A. S. Holevo, and C. M. Caves, eds., (Plenum Press, New York, 1997).
[25] B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainman, J. Mod. Opt. **44,** 953–961 (1997).
[26] B. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, Phys. Rev. A **57,** 2383–2398 (1998).